Introduction à la cryptographie

Comment est apparue la cryptographie?

De tout temps, les codes ont existé. Ils ont d'abord servi à **retranscrire des idées**, à **écrire un langage**. l'homme a perçu le besoin **de cacher, de dissimuler** des informations personnelles ou confidentielles, et cela bien avant l'ère informatique.
Mais avec ces nouveaux moyens de communication est arrivé la **nécessité** de **protéger le contenu** de certains messages des inévitables curieux.

Ainsi est apparue la **cryptographie= la science ou l'art de dissimuler ou cacher des messages ou textes ou...etc (le rendre inutilisable...)**.
Autrement dit, la science qui crée des **cryptogrammes (à l'aide de codes secrets pour chiffrer et déchiffrer)**.

Essentiellement, il y'a deux méthodes fondatentales pour la cryptographie classique
<
seconde guerre mondiale: transposition, substitution .
Stéganographie: Contrairement à la cryptographie, qui **chiffre** des messages de manière à les rendre incompréhensibles, la stéganographie (en grec «l'écriture couverte») **cache** les messages dans un support, par exemple des images ou un texte qui semble anodin (comme l'alphabet bilitère de Francis Bacon ou les fameuses lettres de George Sand). L' idée est la même pour les grilles de Cardan et le «barn code»: on noie le message dans un autre et seuls certains mots doivent être lus pour découvrir le texte caché.

LEXIQUE:

Cryptogramme: Message chiffré ou codé.
Cryptographie: Discipline incluant les principes, les moyens et les méthodes de transformation des données, dans le but de masquer leur contenu, d'empêcher leur modification ou leur utilisation illégale.
Cryptologie: Science des messages secrets. Se décompose en cryptographie et cryptanalyse.
Le mot cryptologie est souvent utilisé comme synonyme de cryptographie.
Chiffre: Ensemble de procédés et ensemble de symboles (lettres, nombres, signes, etc.) employés pour remplacer les lettres du message à chiffrer. On distingue généralement les chiffres à transposition et ceux à substitution.
Chiffrer=Crypter: Transformer un message afin qu'il ne soit lisible qu'à l'aide d'une clef.
Décrypter: Parvenir à restaurer des données qui avaient été chiffrées, donc à leur faire retrouver leur état premier ("en clair"), sans disposer des clefs théoriquement nécessaires.
Clef: Dans un système de chiffrement, elle correspond à un nombre, un mot, une phrase, etc. qui permet, grâce à l'algorithme de chiffrement, de chiffrer ou de déchiffrer un message.
Double clef (chiffre à): Autre terme pour chiffre polyalphabétique.
....etc

Sources utilisées pour ce tableau

Favoris:

- **Singh**: Simon Singh, "Histoire des codes secrets", LC Lattès, 1999.
- **Kahn**: David Kahn, "La guerre des codes secrets", InterEditions, 1980.

Autres:

- **Diffie**: Whitfield Diffie and Martin Hellman, "New Directions in Cryptography", IEEE Transactions on Information Theory, Nov 1976.
- **Cerf**: Nicolas Cerf, Nicolas Gisin, "Les promesses de l'information quantique", La Recherche 327, Janvier 2000, pp. 46-53
- **Garfinkel**: Simson Garfinkel, "PGP: Pretty Good Privacy", O'Reilly & Associates, Inc., 1995.
- **IACR90**: Proceedings, EUROCRYPT '90; Springer Verlag.
- **Newton**: David E. Newton, "Encyclopedia of Cryptology", ABC-CLIO, 1998
- **RSA**: Rivest, Shamir and Adleman, "A method for obtaining digital signatures and public key cryptosystems", Communications of the ACM, Feb. 1978, pp. 120-126.
- .....etc

Entre 2000 avant et 1000 après. J.-C.

Naissance spontanée de la cryptographie : Les écritures secrètes semblent être nées spontanément dès que, dans un pays, une partie importante de la population a su lire.

DATES	SOURCES	IMAGES	COMMENTAIRES
Environ 1900 avant J.-C.	Kahn p. 1		Un scribe égyptien a employé des hiéroglyphes non conformes à la langue correcte dans une inscription. Kahn le qualifie de premier exemple documenté de cryptographie écrite. *Scribe égyptien*= Un copiste, un homme qui gagne sa vie à écrire, à copier.
1500 avant J.-C.	Kahn p. 5		Une tablette mésopotamienne contient une formule chiffrée pour la fabrication de vernis pour les poteries. Il a été inscrite sur cette tablette par un potier babylonien qui voulait dissimuler la recette de son succès.
600-500 avant J.-C.	Kahn p. 6, Singh p. 42		Des scribes hébreux mettant par écrit le livre de Jérémy ont employé un simple chiffre de substitution connu sous le nom d'Atbash. C'était un des quelques chiffres hébreux de cette époque. *Scribe juifs*=ceux qui enseignoient la Loi de Moïse, et qui l'interprétoient au peuple.

487 avant J.-C.	Kahn p. 9, Singh p. 24		Les grecs emploient un dispositif appelé la "scytale" - un bâton autour duquel une bande longue et mince de cuir était enveloppée et sur laquelle on écrivait le message. Le cuir était ensuite porté comme une ceinture par le messager. Le destinataire avait un bâton identique permettant d'enrouler le cuir afin de déchiffrer le message.
Environ 150 avant J.-C.	Kahn p. 10		L'historien grec **Polybe** (env. 200-125 av. J.-C.) invente le carré de Polybe, dont s'inspireront plus tard bien des cryptosystèmes.
60-50 avant J.-C.	Kahn p. 11, Singh pp. 25-26		**Jules César** (100-44 avant J.-C.) employait une substitution simple avec l'alphabet normal (il s'agissait simplement de décaler les lettres de l'alphabet d'une quantité fixe) dans les communications du gouvernement. Ce chiffre était moins robuste qu'Atbash, mais à une époque où très peu de personnes savaient lire, cela suffisait. César écrivait aussi parfois en remplaçant les lettres latines par les lettres grecques.
5e siècle ?	Singh, pp. 24-25		Le **Kama-sutra** est un texte écrit au 5e siècle par le brahmane Vatsayayana, mais fondé sur des manuscrits du 4e siècle avant J.-C. Le Kama-sutra recommande que les femmes apprennent 64 arts, entre autres cuisiner, s'habiller, masser et élaborer des parfums. La liste comprend aussi des domaines moins évidents, comme la prestidigitation, les échecs, la reliure et la tapisserie. Le numéro 45 de la liste est le **mlecchita-vikalpa**, l'art de l'écriture secrète, qui doit leur permettre de dissimuler leurs liaisons.
855	Kahn p. 15		**Abu Bakr ben Wahshiyya** publie plusieurs alphabets secrets utilisés à des fins de magie, dans son livre "Kitab shauk almustaham fi ma'arifat rumuz al aklam" (Le livre de la connaissance longuement désirée des alphabets occultes enfin dévoilée).
9e siècle	Singh, pp. 33-35		**Abu Yusuf Ya'qub ibn Is-haq ibn as-Sabbah Oòmran ibn Ismaïl al-Kindi** rédige le plus ancien texte connu décrivant la technique de décryptement appelée analyse des fréquences.

Entre 1000 et 1800 : l'éveil de l'occident.

Jusque-là largement devancé par la science arabe, l'Occident développe la cryptographie et la cryptanalyse.

DATES	SOURCES	IMAGES	COMMENTAIRES
1226	Kahn p.19		À partir de 1226, une timide cryptographie politique apparaît dans les archives de Venise, où des points ou des croix remplacent les voyelles dans quelques mots épars.
Environ 1250	Kahn p. 13, Singh p. 42		**Roger Bacon** a non seulement décrit plusieurs chiffres, mais il a aussi écrit : "Il est fou celui qui écrit un secret de toute autre manière que celle qui le soustrait à la connaissance du vulgaire".
1379	Kahn p. 19-20		**Gabriel de Lavinde** compose un recueil de clefs, dont plusieurs combinent code et substitution simple. En plus d'un alphabet de chiffrement, souvent avec des nulles, on trouve un petit répertoire d'une douzaine de noms communs et de noms propres avec leurs équivalents en bigrammes. C'est le premier exemple d'un procédé qui devait prévaloir pendant 450 ans en Europe et en Amérique: le

			nomenclateur.
1392	Singh p. 42		Dans un ouvrage intitulé "L'équatorial des Planètes", qui décrit le fonctionnement d'un instrument astronomique, **Geoffrey Chaucer**, a incorporé six courts cryptogrammes écrits de sa propre main.
1412	Kahn p. 16-18		La science arabe en matière de cryptologie est exposée dans la *subh al-a sha*, une énorme encyclopédie en 14 volumes, écrite pour fournir à la bureaucratie une connaissance exhaustive de toutes les principales branches du savoir. Son auteur, qui vivait en Egypte, était **Abd Allah al-Qalqashandi**. La section intitulée "De la dissimulation des informations secrètes dans les lettres" comporte deux parties, l'une traitant des représentations symboliques et du langage convenu, l'autre des encres invisibles et de la cryptologie.
1466-7	Kahn pp. 20-23, Singh pp. 61-62		**Leon Battista Alberti** invente et publie le premier chiffre polyalphabétique. Il conçoit un cadran chiffrant pour simplifier le processus. Cette classe de chiffre n'a pas été apparemment cassée jusqu'aux années 1800. Alberti a aussi écrit largement sur l'état de l'art dans des chiffres, en plus de sa propre invention. Ces chiffres polyalphabétiques étaient beaucoup plus robustes que le nomenclateur qu'utilisaient les diplomates de l'époque. Alberti inventa aussi le surchiffrement codique. Mais le génie d'Alberti était trop en avance sur son temps et ce n'est que 400 ans plus tard, vers la fin du 19e siècle, que les principales puissances mondiales commencèrent à surchiffrer leurs codes mais par des procédés bien plus simples.
1474	Wikipedia		Un contemporain d'Alberti, **Sicco Simonetta**, cryptanalyste au service du Duc de Milan, écrit *Liber Sifrorum*, un traité de cryptanalyse.
1506	Kahn pp. 23-24		Le premier grand cryptanalyste européen fut peut-être **Giovanni Soro**, nommé secrétaire chiffreur en 1506. Il devint secrétaire du chiffre de Venise. Le Vatican lui-même testa ses chiffres sur Soro, qui les perça à jour une première fois. Le Pape envoya d'autres textes chiffrés à Soro afin de savoir si le meilleur cryptanalyste pouvait battre son chiffre. Soro renvoya les textes en écrivant qu'il n'avait pas réussi à les déchiffrer mais on ne sut jamais s'il avait dit la vérité, ou s'il avait menti pour pouvoir décrypter sans difficultés tout message émanant des autorités pontificales...
1518	Kahn pp. 26-28, Singh p. 62		**Jean Trithème** a écrit le premier livre imprimé sur la cryptologie. Il a inventé un chiffre stéganographique dans lequel chaque lettre est représentée par un mot. La série résultante de mots ressemble à une prière. Il a aussi décrit des chiffres polyalphabétiques sous la forme désormais standard de tables de substitution rectangulaires.
1550 env.	Kahn pp. 37-38		**Jérôme Cardan** invente le premier procédé autoclave, mais ce système est imparfait et c'est finalement un autre procédé qui porte son nom. La grille de Cardan consiste en une feuille de matériau rigide dans laquelle ont été découpées, à des intervalles irréguliers, des fenêtres rectangulaires de la hauteur d'une ligne d'écriture et de longueur variable. Le chiffreur écrit le texte dans les fenêtres, puis retire le cache et comble les espaces vides avec un texte anodin. Le destinataire pose la même grille sur le texte crypté pour lire le message caché.
1553	Kahn pp. 34-35		**Giovan Batista Belaso** fait paraître un petit livre intitulé *La cifra del. Sig. Giovan Batista Belaso*. Il y proposait, pour le chiffrement en substitution polyalphabétique, l'emploi de clefs littérales, faciles à garder en mémoire et à changer. Il les appelait "mot de passe". Les clefs littérales furent immédiatement adoptées et l'innovation de Belaso est à l'origine de certains systèmes actuels très complexes où plusieurs clefs - et non pas une seule - sont utilisées et changées de façon irrégulière.
1563	Kahn pp. 35-36		**Giovanni Battista Della Porta** écrit *De Futivis Literarum Notis*. Ces quatre livres, traitant respectivement des chiffres anciens, des chiffres modernes, de la cryptanalyse, des caractéristiques linguistiques qui favorisent le déchiffrement, représentent la somme des connaissances cryptologiques de l'époque. Parmi les procédés modernes, dont beaucoup sont de son inventions, apparaît la première substitution bigrammatique: deux lettres sont représentées par un seul symbole. Il inventa aussi le premier chiffre polyalphabétique. Il fut le premier à classer les

			deux principes cryptographiques majeurs: la substitution et la transposition.
1578			**Marins**, un des décrypteurs de la république de Venise, fait paraître *Del mondo di extrazar le cifre*.
1585	Kahn pp. 39-42, Singh pp. 62-67		**Blaise de Vigenère** écrit son *Traicté des chiffres ou secrètes manières d'escrire*. Il présente entre autres un tableau du type **Trithème**, que l'on dénomme aujourd'hui à tort carré de Vigenère. On considéra longtemps ce chiffre comme indécryptable, légende si tenace que même en 1917, plus de cinquante après avoir été cassé, le Vigenère était donné pour "impossible à décrypter" par la très sérieuse revue *Scientific American*.
1623	Kahn pp. 359-364		**Sir Francis Bacon** (que l'on soupçonne fortement d'être William Shakespeare) est l'inventeur d'un système stéganographique qu'il exposa dans *De dignitate et augmentis scientiarum*. Il appelait son alphabet bilitère, car il utilisait un arrangement des deux lettres A et B en groupes de cinq.
1691	Kahn pp. 46-50, Singh p. 71		**Antoine Rossignol** et son fils Bonaventure élabore le **Grand Chiffre** de Louis XIV. Il tomba en désuétude après la mort de ses inventeurs et ses règles précises furent rapidement perdues. Le grand Chiffre était si robuste qu'on était encore incapable de la lire à la fin du 19e siècle, jusqu'à **Bazeries**.

Entre 1800 et 1970: l'essor des communications.

Les nouvelles techniques de communications (moyens de transports rapides, journaux, télégraphe, télégraphie sans fil) donne une nouvelle impulsion à la cryptologie. Les guerres modernes utilisent abondamment les télécommunications; l'interception devient simple et le décryptement des informations devient vital. La cryptologie entre dans son ère industrielle.

DATES	SOURCES	IMAGES	COMMENTAIRES
Les années 1790	Kahn pp. 154-156		**Thomas Jefferson**, invente son cylindre chiffrant, si bien conçu qu'après plus d'un siècle et demi de rapide progrès technique, il était encore utilisé. C'était sûrement le moyen de chiffrement le plus sûr de l'époque, et pourtant il fut classé et oublié. Il fut réinventé en 1891 par Etienne Bazeries, qui ne parvint pas à le faire adopter par l'armée française. L'armée américaine mit en service un système presque identique en 1922.
1854	Kahn pp. 64-68, Singh pp. 401-402		**Charles Wheatstone**, un des pionniers du télégraphe électrique, invente le chiffre Playfair, du nom de son ami Lyon Playfair qui a popularisé ce chiffre.
1857			Après la mort de **l'amiral Sir Francis Beaufort**, son frère publie le chiffre de Beaufort (une variante du chiffre de Vigenère).
1854	Singh pp. 79-93		**Charles Babbage** casse le chiffre de Vigenère, mais sa découverte resta ignorée, car il ne la publia pas. Ce travail ne fut mis en lumière qu'au 20e siècle, lors de recherches effectuées sur l'ensemble des papiers de Babbage.

1861	Kahn pp. 69-70, Singh p. 93		**Friedrich W. Kasiski** publie *Die Geheimshriften und die Dechiffrierkunst* (les chiffres et l'art du déchiffrement), qui donne la première solution générale pour le déchiffrement d'un chiffre polyalphabétique à clefs périodique, marquant ainsi la fin de plusieurs siècles d'invulnérabilité du chiffre de Vigenère.
1891	Kahn pp. 71-76, Singh pp. 72-74		Le commandant **Étienne Bazeries** produit son cryptographe cylindrique. Il était composé de vingt disques portant chacun vingt-cinq lettres. Il ne sera jamais employé par l'armée française. Bazeries fut aussi le premier à déchiffrer le Grand chiffre de Louis XIV.
1917	Kahn pp. 374-377		**Gilbert S. Vernam**, travaillant pour AT&T, a inventé une machine de chiffre polyalphabétique pratique capable d'employer une clef qui est totalement aléatoire et ne se répète jamais - un masque jetable. C'est seul le chiffre, dans nos connaissances actuelles, dont on a prouvé qu'il était indécryptable en pratique **et** en théorie. Ce procédé ne fut cependant jamais utilisé par l'armée car il exigeait de devoir produire des millions de clefs différentes (une par message), ce qui est impraticable. Par contre, il fut utilisé par les diplomates allemands dès 1921.
1918	Kahn pp. 140-143, Singh pp. 117-119 & pp. 403-404		Le système ADFGVX a été mis dans le service par les Allemands à la fin de la première guerre mondiale. Il a été cassé par le lieutenant français **Georges Painvin**.
1918	Kahn p. 379, Singh pp. 142-157	Scherbius	**Arthur Scherbius** fait breveter sa machine à chiffrer Enigma. Le prix d'un exemplaire s'élevait à 20'000 livres en valeur actuelle. Ce prix sembla décourager les acheteurs potentiels. Il est à noter que trois autres inventeurs, dans trois pays, avaient, chacun de son côté et presque simultanément, eu l'idée d'une machine basée sur des rotors: **Hugo Alexandre Koch**, **Arvid Gerhard Damm** et **Edouard Hugh Hebern**.
1925	Newton, pp. 129-130		**Boris Caesar Wilhelm Hagelin** (1892-1983) propose à l'armée suédoise la machine B-21, qui fut pendant une décennie la machine la plus compacte capable d'imprimer des messages chiffrés. Pendant la seconde guerre mondiale, les Alliés fabriquèrent une autre machine de Hagelin, la Hagelin C-36 (appelée M-209 aux États-Unis), à 140 000 exemplaires. Après la guerre, Boris Hagelin créa à Zoug, en Suisse, **Crypto AG**, qui est aujourd'hui encore l'un des principaux fabricants d'équipements cryptographiques. Crypto AG =develops and produces security systems for all common information and communication technologies.
1929			**Lester S. Hill** publie son article "Cryptography in an Algebraic Alphabet", dans *American Mathematical Monthly*, **36**, 1929, pp. 306-312. Il y décrit le chiffre qui porte son nom. C'est un chiffre polygraphique où l'on utilise des matrices et des vecteurs.
1931	Kahn pp. 167-175		**Herbert O. Yardley** publie *The American Black Chamber*, un des livres les plus célèbres sur la cryptologie. Il décrypta entre autres les codes japonais (avant leur machine PURPLE).
1933-45	Kahn pp. 257-265, Singh pp. 142-207	Turing	La machine Enigma ne fut pas un succès commercial mais elle fut reprise et améliorée pour devenir la machine cryptographique de l'Allemagne nazie. Elle a été cassée par le mathématicien polonais **Marian Rejewski**, qui s'est basé seulement sur un texte chiffré et une liste des clefs quotidiennes obtenues par un espion. Pendant la guerre, les messages furent régulièrement décryptés par **Alan Turing, Gordon Welchman** et d'autres à Bletchley Parc, en Angleterre, à l'aide des premiers ordinateurs (les fameuses **bombes**).

1940	Kahn pp. 175-180		**William Frederick Friedman**, plus tard honoré comme le père de la cryptanalyse américaine, à la tête de son équipe du Signal Intelligence Service (S.I.S.), réussit le décryptement de la machine à chiffrer japonaise PURPLE. Avec sa femme, il s'intéressa beaucoup aux chiffres shakespeariens, et, pendant la prohibition, ils déchiffrèrent les codes des trafiquants.

La cryptologie moderne : de 1970 à nos jours.

Les ordinateurs et le réseau Internet font entrer la cryptologie dans son ère moderne. La grande invention de ces dernières décennies fut la cryptographie à clefs publiques. Le futur sera peut-être la cryptographie quantique, définitivement indécryptable.

DATES	SOURCES	IMAGES	COMMENTAIRES
1970	Singh pp. 270-272		Au début des années 1970, **Horst Feistel** a mené un projet de recherche à l'IBM Watson Research Lab qui a développé le chiffre **Lucifer**, qui inspira plus tard le chiffre DES et d'autres chiffres. Un avantage de ce type d'algorithmes est que chiffrement et déchiffrement sont structurellement identiques.
1976	Diffie, Singh pp. 274-294	Diffie Hellman	**Whitfield Diffie** et **Martin Hellman** publient *New Directions in Cryptography*, introduisant l'idée de cryptographie à clef publique. Ils donnent une solution entièrement nouvelle au problème de l'échange de clefs. Ils avancent aussi l'idée d'authentification à l'aide d'une fonction à sens unique. Ils terminent leur papier avec une observation : "L'habileté dans la cryptanalyse a toujours été lourdement du côté des professionnels, mais l'innovation, en particulier dans la conception des nouveaux types de systèmes cryptographiques, est venue principalement d'amateurs."
Novembre 1976	Singh pp. 272-273		**DES**, pour Data Encryption Standard ("standard de cryptage de données"), est un algorithme très répandu à clef privée dérivé du chiffre Lucifer de Feistel (de chez IBM) dans sa version à 64 bits. Il sert à la cryptographie et l'authentification de données. Il a été jugé si difficile à percer par le gouvernement des Etats-Unis qu'il a été adopté par le ministère de la défense des Etats-Unis qui a contrôlé depuis lors son exportation. Cet algorithme a été étudié intensivement et est devenu l'algorithme le mieux connu et le plus utilisé dans le monde à ce jour. Bien que DES soit très sûr, certaines entreprises préfèrent utiliser le "triple-DES", qui n'est rien d'autre que l'algorithme DES appliqué trois fois, avec trois clés privées différentes.
Avril 1977	Singh pp. 295-302	Rivest Shamir	**RSA** signifie Rivest-Shamir-Adleman, en l'honneur de ses trois inventeurs : **Ron Rivest**, **Adi Shamir** et **Leonard Adleman** qui l'ont inventé en 1977. Le brevet de cet algorithme appartient à la société américaine RSA Data Security, qui fait maintenant partie de Security Dynamics et aux Public Key Parteners, (PKP à Sunnyvale, Californie, Etats-Unis) qui possèdent les droits en général sur les algorithmes à clé publique. RSA est un algorithme à clé publique qui sert aussi bien à la cryptographie de documents, qu'à l'authentification. Grâce au fait qu'il était à clé publique, et au fait qu'il était très sûr, l'algorithme RSA est devenu un standard de facto dans le monde. L'implémentation fut achevée en 1978 par Rivest, Shamir et Adleman. Depuis, ce système de chiffrement est appelé RSA, qui sont les initiales de ces trois chercheurs.

		Adleman	
1978	RSA		L'algorithme **RSA** est publié dans les Communications de l'ACM.
1990	IACR90		**Xuejia Lai** et **James Massey** publient *A Proposal for a New Block Encryption Standard*, un algorithme de cryptage des données International (l'**IDEA**: **I**nternational **D**ata **E**ncryption **A**lgorithm) - pour remplacer le DES. L'IDEA emploie une clef de 128 bits et utilise des opérations convenant bien à tout type d'ordinateurs, permettant donc une programmation plus efficace. Il s'agit d'un des meilleurs algorithmes de chiffrement, si ce n'est le meilleur. Personne n'a dévoilé à ce jour avoir cassé d'une manière ou d'une autre le moindre bloc de texte chiffré par IDEA. Il est actuellement exploité par la société Mediacrypt.
1990	IACR90, Singh pp. 367-378	Bennett	**Charles H. Bennett** et **Gilles Brassard** publient leurs résultats expérimentaux sur la Cryptographie Quantique, qui emploie des photons pour communiquer un flot de bits qui serviront de clefs pour un cryptage de type Vernam (ou d'autres utilisations). En supposant que les lois de la mécanique quantique se vérifient, la Cryptographie Quantique offre non seulement le secret, mais permet aussi de savoir si la ligne a été écoutée. Comme inconvénient, la QC exige actuellement un câble en fibres optiques entre les deux correspondants.
1991	Garfinkel, Singh pp. 319-343		**Phil Zimmermann** sort sa première version de **PGP** (Pretty Good Privacy) en réponse à la menace du FBI d'exiger l'accès au message clair des citoyens. PGP offre une haute sécurité au citoyen et cela gratuitement. PGP est en effet un freeware et est devenu rapidement une norme mondiale. Pretty Good Privacy (PGP)=programme gratuit de protection du courrier électronique conçu en 1991 par Philip Zimmermann . Sa philosophie est que tout individu a droit à la confidentialité, notamment les organisations des droits de l'homme dans des pays soumis à la dictature. C'est dans cette optique qu'il a créé PGP et qu'il l'a mis à disposition gratuitement sur Internet.Cela lui a valu de sérieux ennuis avec la justice américaine, car les logiciels de cryptage sont considérés comme du matériel de guerre et sont interdits à l'exportation.
1995	Cerf		**Nicolas Gisin** et son équipe distribuent des clefs secrètes à l'aide d'un câble optique de 25 kilomètres sous le lac Léman en codant les q-bits par la polarisation de photons (cryptographie quantique). La distance est le prochain obstacle que devront franchir les chercheurs, car le dispositif ne peut excéder 50 à 60 km, selon leurs estimations.
Août 1999	LIX		11 sites répartis dans 6 pays factorisent le premier nombre ordinaire de 155 chiffres décimaux (512 bits). Un tel nombre aurait pu servir de clef dans un système de chiffrement moderne de type RSA, qui est utilisé dans le commerce électronique. Un tel record remet en question l'utilisation de clefs trop petites dans de tels systèmes.

Références

- La cryptographie (par David Blanc)
- A Short History of Cryptography (by Fred Cohen)
- CME's Cryptography Timeline (by Carl Ellison)
- Wikipédia : Histoire de la cryptologie

Univesrité d'Evry Val d'essonne 2008-2009

UEL: Histoire de la cryptologie

TD1: Codes Hebreux, cesar, Polybe et la scytale.

Nous avons adapté ci-dessous les chiffres Atbash, Albam et Atbah à notre alphabet occidental actuel.

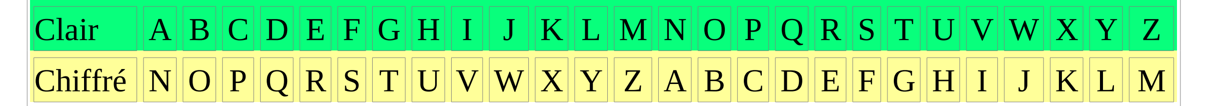
Le chiffre Atbash

Le chiffre Atbash consiste simplement à inverser l'ordre des lettres de l'alphabet. Il est à remarquer que le mot "Atbash" dérive du système qu'il désigne, puisqu'il est composé à partir des lettres **a**leph, **t**au, **b**eth et **sh**in, les deux premières et les deux dernières de l'alphabet hébreux.

Clair	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Chiffré	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A

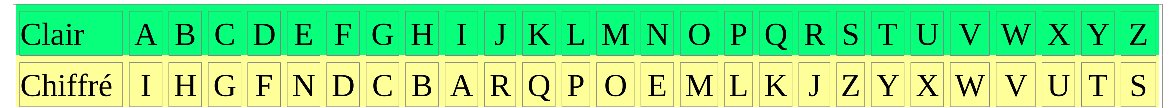
Le chiffre Albam

Ce chiffre décale les lettres de l'alphabet de 13 positions. Il est réapparu en 1984 sous le nom de ROT13 dans un programme permettant de lire les "News" de USENET.



Clair	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Chiffré	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M

Le chiffre Atbah



Clair	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Chiffré	I	H	G	F	N	D	C	B	A	R	Q	P	O	E	M	L	K	J	Z	Y	X	W	V	U	T	S

Ces trois chiffres sont réversibles, c'est-à-dire qu'un message chiffré deux fois avec le même chiffre redonnera le message en clair.

Surchiffrement

Le surchiffrement consiste à chiffrer un message qui a déjà été chiffré d'une autre manière. On peut par exemple chiffrer d'abord avec le chiffre Atbash, puis avec le chiffre Albam. On peut rapprocher cela d'une composition de fonctions et l'écrire Albam(Atbash).

Clair	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Atbash	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A
Albam(Atbash)	M	L	K	J	I	H	G	F	E	D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N
Atbah(Albam(Atbash))																										

Exercice 1:

- Remplissez la dernière ligne du tableau ci-dessus.
- Le message suivant a été chiffré successivement avec les chiffres Atbash, Albam et Atbah. Essayez de le décrypter.

JTZXJ ASAER ARAQD NBBWA WZSIA XXOCA XZWQD NBBWA

- Est-ce que l'ordre de chiffrement est important ?A**tbash(Atbah) = Atbah(Atbash) ?**

Exercice 2 (Scytale) :

Décryptez ce message secret avec une **scytale**: **vvt goerlruzo'as uam rvnmaeéae**

Exercice 3 (Polybe) :

Chiffrement

Chiffrez **à la main** le texte suivant avec le carré de Polybe (sans mot-clef):

> L'homme est un ange déchu qui se souvient du ciel.

Vérifiez votre cryptogramme avec le programme ci-dessus.

Déchiffrement

Déchiffrez **à la main** le texte suivant avec le carré de Polybe en utilisant le mot-clef "Blaise Pascal":

> **122115 141221 412321 214521 44412 112242 123211 521152 213232 115144 125144 114153 521252 544131 421**

Exercice 4 (Cesar):

Chiffrement



Chiffrez **à la main** le texte suivant avec le chiffre de César en décalant les lettres de 7 rangs vers la gauche:

> La rue assourdissante autour de moi hurlait.
> Longue, mince, en grand deuil, douleur majestueuse.

Vérifiez votre cryptogramme avec le programme ci-dessus.

Déchiffrement

Déchiffrez **à la main** le texte ci-dessous chiffré avec le chiffre de César en décalant les lettres de 7 rangs vers la gauche:

> BULML TTLWH ZZHKB ULTHP UMHZA BLBZL ZVBSL CHUAI HSHUJ HUASL MLZAV ULASV BYSLA

L'analyse des fréquences

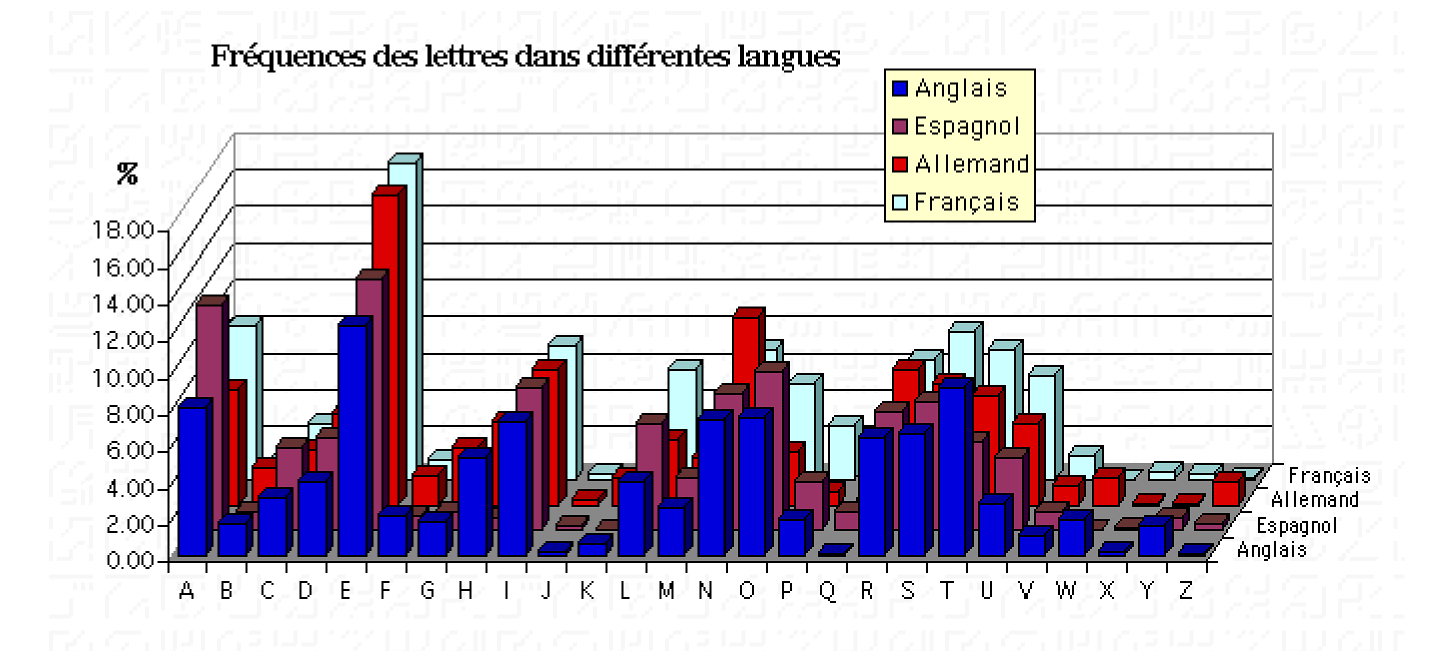


Un des moyens les plus simples de chiffrer un message est de remplacer chaque lettre par une autre (ou un autre symbole). Par sa simplicité et par sa force, ce système a dominé la technique des écritures secrètes pendant tout le premier millénaire. Il a résisté aux cryptanalystes jusqu'à ce que le savant arabe Abu Yusuf Ya'qub ibn Is-haq ibn as-Sabbah Oòmran ibn Ismaïl **al-Kindi** (ouf!) mette au point, au IXème siècle, une technique appelée analyse des fréquences.

Al-Kindi (801-873) rédige sa méthode dans son plus important traité intitulé *Manuscrit sur le déchiffrement des messages cryptographiques.* C'est le premier manuscrit connu faisant mention des fréquences d'apparition des lettres (voir la première page de ce manuscrit ci-contre). Il explique que « la façon d'élucider un message crypté, si nous savons dans quelle langue il est écrit, est de nous procurer un autre texte en clair dans la même langue, de la longueur d'un feuillet environ, et de compter alors les apparitions de chaque lettre.
Ensuite, nous nous reportons au texte chiffré que nous voulons éclaircir et relevons de même ses symboles. Nous remplaçons le symbole le plus fréquent par la lettre première (la plus fréquente du texte clair), le suivant par la deuxième, le suivant par la troisième, et ainsi de suite jusqu'à ce que nous soyons venus à bout de tous les symboles du cryptogramme à résoudre ».

Cette technique ne fonctionne bien que si le cryptogramme est suffisamment long pour avoir des moyennes significatives.

Les pages suivantes indiquent les fréquences en français, en allemand, en anglais en espagnol et en russe. L'histogramme ci-dessous permet de comparer les fréquences dans les quatre premières langues (qui utilisent les lettres latines).



Référence

- Poe Edgar Allan, Le Scarabée d'or. Edgar Poe expose dans ce texte, devenu un classique, l'analyse des fréquences.

Le code de Mary Stuart



Au matin de 15 octobre 1586, **Marie Stuart** prénètre dans la salle d'audience bondée du château de Fotheringhay. Elle est jugée pour trahison, accusée d'avoir pris part à un complot tendant à assassiner la reine Elizabeth, afin de s'emparer elle-même de la couronne d'Angleterre. **Sir Francis Walsingham**, Premier secrétaire de la reine Elizabeth, avait déjà fait arrêter les autres conspirateurs, avait obtenu leurs aveux et les avait fait exécuter. Malheureusement pour Mary, Walsingham était aussi le chef de l'espionnage anglais. Il avait intercepté les lettres de Mary aux conspirateurs et connaissait l'homme capable de les déchiffrer: **Thomas Phelippes**.
Le chiffre utilisé n'était pas simplement une substitution, mais plutôt un nomenclateur, comme le montre la figure ci-dessous. Il était constitué de 23 symboles qui remplaçaient les lettres de l'alphabet (sauf j, v et w), ainsi que de 36 symboles représentant des mots ou des phrases. Il y avait en outre quatre nulles et un symbole qui signifiait que la lettre suivante était une lettre doublée.

a b c d e f g h i k l m n o p q r s t u x y z

Nulles ff. ⊢ . ⊣ . d .   Dowbleth

and for with that if but where as of the from by

so not when there this in wich is what say me my wyrt

send lr̃e receave bearer I pray you Mte your name myne

Ce code était trop simple pour résister à un des meilleurs cryptanalystes d'Europe.
Mary Stuart avait été arrêtée dix-huit ans plus tôt, pour le meurtre de son mari. En fait, c'était surtout un prétexte car beaucoup de sujets considéraient que c'était elle la souveraine légitime de l'Angleterre et non Elizabeth. Toutes les lettres que Mary écrivait et recevait depuis sa semi-captivité étaient interceptées, ouvertes, recopiées avant d'être acheminées à leur destinataire. Walsingham eut l'idée, pour démanteler complètement le réseau, d'introduire de faux post-sciptum dans les lettres adressées à Mary pour qu'elle écrive les noms des conspirateurs. Trop confiante en son code, elle le fit. Tous ses complices furent arrêtés et sauvagement exécutés. Elle-même mourut décapitée le 8 février 1857 (voir image ci-dessous).



Référence

- Singh Simon, **Histoire des codes secrets**, Editions JC Lattès, 1999, pp. 17-59

Principes de Kerckhoffs

Pour qu'une méthode de cryptographie destinée à régler pour un temps illimité la correspondance secrètes: il faut un système remplissant certaines conditions exceptionnelles, conditions que je résumerai sous les six chefs suivants:

1. Le système doit être matériellement, sinon mathématiquement, indéchiffrable;
2. Il faut qu'il n'exige pas le secret, et qu'il puisse sans inconvénient tomber entre les mains de l'ennemi;
3. La clef doit pouvoir en être communiquée et retenue sans le secours de notes écrites, et être changée ou modifiée au gré des correspondants;
4. Il faut qu'il soit applicable à la correspondance télégraphique;
5. Il faut qu'il soit portatif, et que son maniement ou son fonctionnement n'exige pas le concours de plusieurs personnes;
6. Enfin, il est nécessaire, vu les circonstances qui en commandent l'application, que le système soit d'un usage facile, ne demandant ni tension d'esprit, ni la connaissance d'une longue série de règles à observer.

Commentaires

Les points 2 et 3 sont les axiomes fondamentaux de la cryptographie:

l'ennemi possède tous les détails de l'algorithme et qu'il ne lui manque que la clef spécifique pour le chiffrement.

Bien que cela ne soit pas toujours le cas dans le monde réel de la cryptanalyse, c'est toujours vrai dans le monde académique de la cryptanalyse.

Ce n'est pas déraisonnable: si l'on ne sait pas casser un algorithme même en sachant comment il fonctionne, on ne sait certainement pas le casser sans cette connaissance.

Un chiffre basé uniquement sur le secret de l'algorithme n'a aucun intérêt, car un jour ou l'autre ce secret sera éventé ou volé.

Par exemple, même si on connaît le "**mode d'emploi**" du **carré de Vigenère,** on ne pourra quand même pas, ou difficilement, décrypter un message si on ne connaît pas la **clef.**

Par contre, le chiffre **Atbash** repose entièrement sur la manière de chiffrer (il n'y a pas de clef).

Exercices

Parmi tous les systèmes cryptographiques que nous avons vus dans ce cours, dites lesquels ne respectent pas les principes de Kerckhoffs et pourquoi.

Niveaux d'attaques

Un des axiomes fondamentaux de la cryptographie, énoncé pour la première fois par Auguste Kerckhoffs au 19e siècle, est que l'ennemi possède tous les détails de l'algorithme et qu'il ne lui manque que la clef spécifique pour le chiffrement.

On appelle attaque une tentative de cryptanalyse.

L'attaque à texte chiffré seulement (ciphertext-only attack)

Le cryptanalyste dispose du texte chiffré de plusieurs messages, tous ayant été chiffrés avec le même algorithme. La tâche du cryptanalyste est de retrouver le plus grand nombre de messages clairs possibles, ou mieux encore de retrouver la ou les clefs qui ont été utilisées, ce qui permettrait de déchiffrer d'autres messages chiffrés avec ces mêmes clefs.

L'attaque à texte clair connu (known-plaintext attack)

Le cryptanalyste a non seulement accès aux textes chiffrés de plusieurs messages, mais aussi aux textes clairs correspondants. La tâche est de retrouver la ou les clefs qui ont été utilisées pour chiffrer ces messages ou un algorithme qui permet de déchiffrer d'autres messages chiffrés avec ces mêmes clefs.

L'attaque à texte clair choisi (chosen-plaintext attack)

Le cryptanalyste a non seulement accès aux textes chiffrés et aux textes clairs correspondants, mais de plus il peut choisir les textes en clair. Cette attaque est plus efficace que l'attaque à texte clair connu, car le cryptanalyste peut choisir des textes en clair spécifiques qui donneront plus d'informations sur la clef (voir l'exercice sur le procédé autoclave).

L'attaque à texte chiffré choisi (adaptative-plaintext attack)

Le cryptanalyste peut choisir différents textes chiffrés à déchiffrer. Les textes déchiffrés lui sont alors fournis. Par exemple, le cryptanalyste a un dispositif qui ne peut être désassemblé et qui fait du déchiffrement automatique. Sa tâche est de retrouver la clef.

> «Deciphering is, in my opinion, one of the most fascinating of arts.»
>
> **Charles Babbage**

Techniques classiques de cryptanalyse

Recherche exhaustive de la clef

Cette technique consiste simplement à essayer toutes les clefs possibles, jusqu'à ce qu'on trouve la bonne. Pour les chiffres à alphabet décalé, comme le chiffre de César, cette recherche est envisageable, puisqu'il y a peu de possibilités (25).

Analyse des fréquences

Dans le cas d'un chiffre monoalphabétique, c'est-à-dire quand l'alphabet est désordonné, ou que chaque lettre est remplacée par un symbole, on peut s'appuyer sur une **analyse des fréquences des lettres** ou des bigrammes.

Technique du mot probable (Cribbing)

Une technique très puissante de décryptement consiste à supposer qu'une séquence de lettres du cryptogramme correspond à un mot que l'on devine (*crib* en anglais). Ce type d'attaque marche aussi bien pour les substitutions simples que pour le chiffre de Vigenère (méthode de Bazeries), les substitutions homophoniques, ou encore le chiffre de Hill. Cette attaque marche aussi contre la grille tournante.
Un dictionnaire des mots croisés peut être très utile, surtout pour décrypter une substitution simple. En voici deux en français disponibles sur le web: Tatout Editions, Dictionnaire de mots croisés Amo, et deux en anglais: Amo's online crossword puzzle dictionary et A2Z Wordfinder.

Test de Friedman

Le **test de Friedman** permet de savoir si l'on a affaire à un chiffre monoalphabétique ou polyalphabétique. Il peut aussi être utilisé pour trouver la longueur de la clef d'un chiffre de Vigenère.

Méthode de Babbage/Kasiski

Pour décrypter un chiffre de Vigenère, Babbage et Kasiski ont mis indépendamment au point une technique qui consiste à repérer des **séquences de lettres qui se répètent** dans le cryptogramme.

Comment reconnaître un chiffre ?

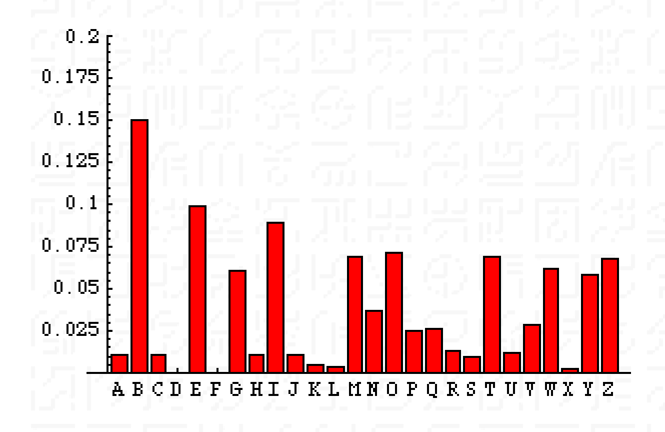
Bien qu'en cryptanalyse théorique on considère que le système de chiffrement est connu, dans la réalité il n'en est pas ainsi.

Nous donnons ici quelques pistes pour reconnaître un chiffre. Il faut cependant être conscient que la liste est loin d'être exhaustive!

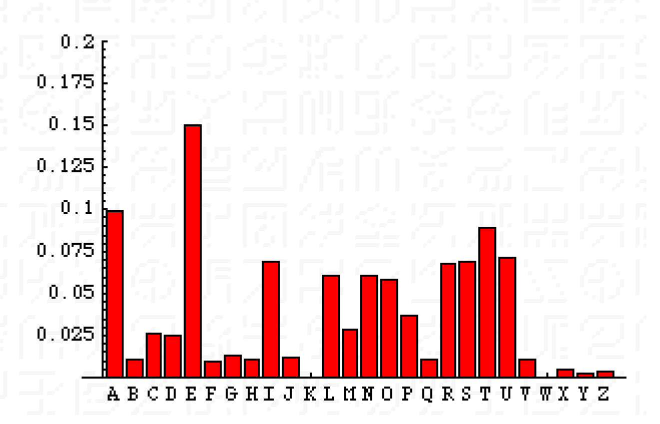
Utilisation des histogrammes

La première choses à faire quand on se trouve devant un message chiffré est de faire des statistiques: nombre de lettres, fréquence de chaque symbole, histogramme.

De l'histogramme on peut déjà dire si c'est une substitution simple, une transposition ou... autre chose.



Exemple d'histogramme caractéristique d'une substitution simple (en français)



Exemple d'histogramme caractéristique d'une transposition (en français)

Si c'est une substitution simple, on doit retrouver des pics, qui correspondront aux lettres les plus fréquentes de la langue (par exemple, dans l'exemple ci-dessus, le E est très probablement

remplacé par le B).

Si c'est une transposition, l'histogramme des lettres sera presque identique à l'histogramme théorique de la langue (les fréquences des lettres seront les mêmes puisqu'elles n'ont pas été remplacées).
Si c'est une substitution simple ou une transposition, on peut aussi deviner la langue d'après les statistiques d'apparition des lettres pour une langue donnée.
Si on retrouve pas de pics, c'est que l'on a affaire à un autre type de chiffrement.



Exemple d'histogramme caractéristique d'un chiffre de Vigenère (en français)

Les symboles utilisés dans le cryptogramme sont des lettres

Soit **n** le nombre de lettres du cryptogramme.

- Si on a un nombre pair de lettres et qu'il n'y a que peu de lettres différentes, on peut les regrouper par deux et les interpréter comme des coordonnées dans une grille (voir le chiffre ADFGVX).
- S'il n'y a que 9 lettres différentes, c'est peut-être un chiffre de Collon.
- Si on a supposé qu'il s'agit d'une transposition, disposer les lettres en **a** lignes et **b** colonnes, avec **a**·**b**=**n**. Essayer ensuite de retrouver la règle de transposition (facile à dire!).
- Si **n** est un carré (p. ex 64, 81, 100, etc), il faut penser à l'utilisation d'une grille carrée, et peut-être d'une grille tournante.
- Il peut aussi s'agir d'une substitution homophonique.
- Le cryptogramme peut aussi avoir été construit à partir d'un système à répertoire.

Les symboles utilisés dans le cryptogramme sont des chiffres

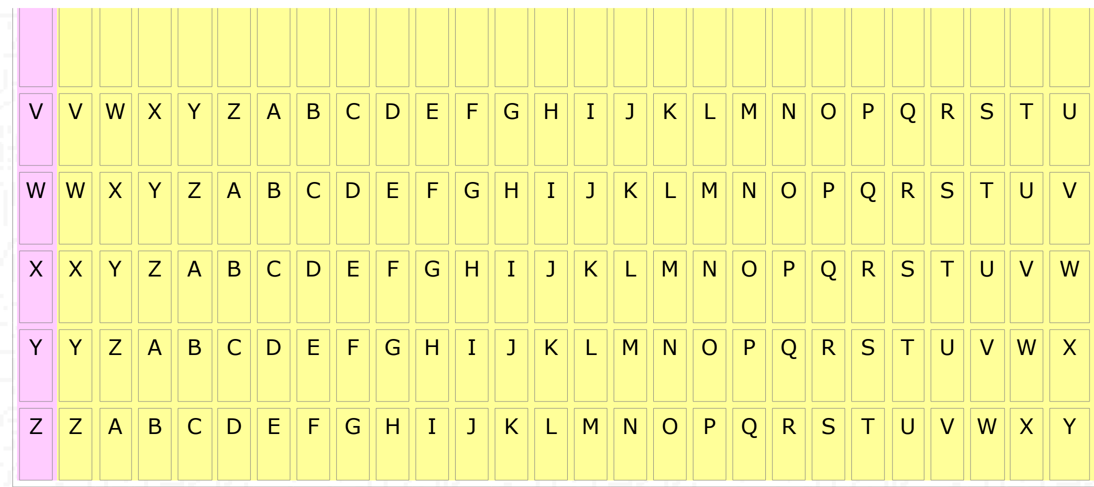
Il y a plusieurs façons d'interpréter ces chiffres. En voici quelques-unes:

- Si les nombres sont compris entre 1 et 26, il s'agit peut-être d'une substitution simple, où un nombre remplace une lettre (par exemple A=1, B=2, etc.). Pour en être sûr, faire un histogramme.
- Si les nombres donnés sont compris entre -25 et 25, il s'agit peut-être de décalages par rapport à l'alphabet usuel ou à un texte qui sert de clef.
- Si on a un nombre pair de chiffres, on peut les regrouper par deux et les interpréter comme des coordonnées dans une grille (voir le chiffre de Polybe).
- Il s'agit aussi peut-être de la position d'une lettre dans un texte qui sert de clef (voir le chiffre du livre)
- Il peut aussi s'agir d'une substitution homophonique.
- Le cryptogramme peut aussi avoir été construit à partir d'un système à répertoire (voir le code Sittler).

Carré de Vigenère

Dans le cinquième volume de ses six livres intitulés *Polygraphiae*, **Jean Trithème** décrit une table qu'il a imaginée et nommée *tabula recta*. Dans cette table, l'alphabet est répété sur 26 lignes, avec un décalage à gauche de une lettre pour chaque nouvelle rangée.
En 1586, **Blaise de Vigenère** reprend cette idée dans son livre *Traicté des chiffres, ou secretes manieres d'escrire*. La dénomination *chiffre de Vigenère* apparut seulement à la fin du 17e siècle, en l'honneur de celui qui lui donna sa forme définitive. Cependant le terme *carré de Vigenère* est erroné, on devrait plutôt dire *carré de Trithème*.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T



V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Version moderne du carré de Vigenère

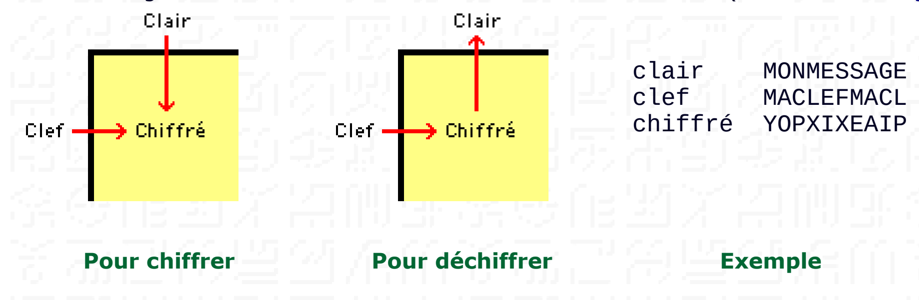
L'emploi du carré de Vigenère est souvent sujet à erreurs: la lecture en est pénible et, à la longue, fatigante. Beaucoup de cryptologues préfèrent se servir d'une "réglette", facile à construire, et d'un maniement plus rapide.

Comment utiliser le carré de Vigenère ?

Voyons maintenant quatre façons d'utiliser ce tableau pour chiffrer des messages.

Vigenère (chiffré = clair + clef)

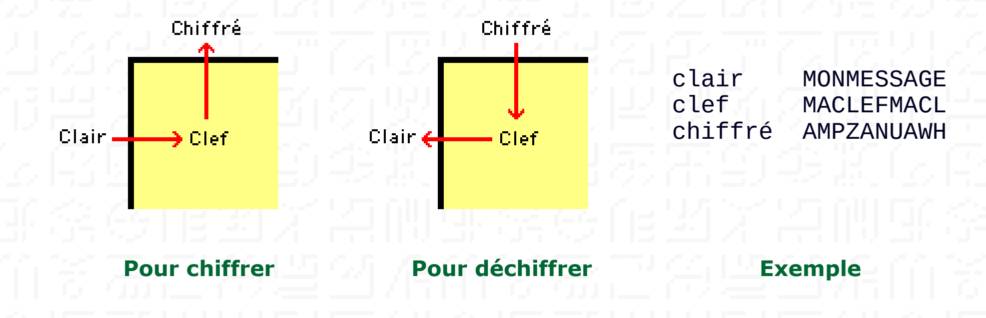
La lettre de la clef est dans la colonne la plus à gauche, la lettre du message clair est dans la ligne tout en haut. La lettre chiffrée est à l'intersection de la ligne de la lettre clef et de la colonne de la lettre claire (voir chiffre de Vigenère).



Pour chiffrer **Pour déchiffrer** **Exemple**

Beaufort (chiffré = clef - clair)

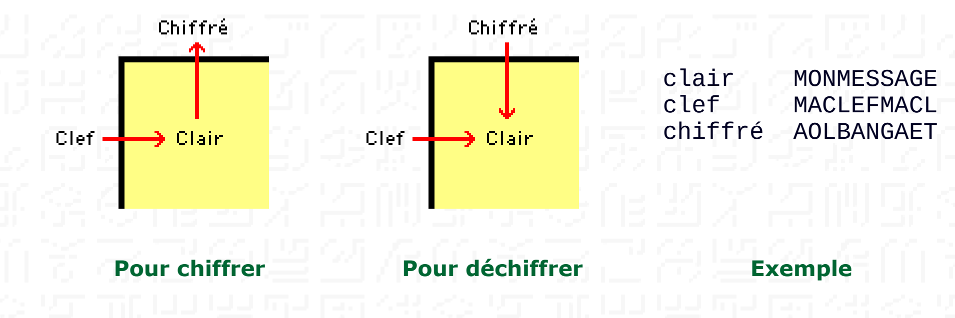
Trouvez la lettre du message clair dans la colonne la plus à gauche, partez ensuite horizontalement vers la droite jusqu'à la lettre de la clef, puis remontez verticalement pour lire la lettre chiffrée dans la ligne tout en haut (voir chiffre de Beaufort).



Pour chiffrer **Pour déchiffrer** **Exemple**

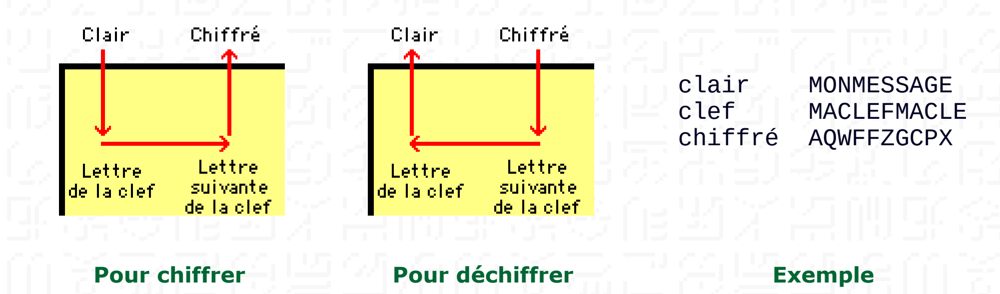
Variante à l'allemande du chiffre de Beaufort (chiffré = clair - clef)

Trouvez la lettre de la clef dans la colonne tout à gauche, partez ensuite horizontalement vers la droite jusqu'à la lettre du message clair, puis remontez verticalement pour lire la lettre chiffrée dans la ligne tout en haut (voir variante à l'allemande du chiffre de Beaufort).



Variante de Rozier

Trouvez la lettre du message clair, descendez jusqu'à trouver la lettre de la clef, puis déplacez-vous horizontalement jusqu'à trouver la lettre suivante de la clef, puis enfin remontez pour lire la lettre chiffrée.



Certains cryptologues ont qualifié ce procédé de "complication illusoire", car il se ramène à un simple chiffre de Vigenère. Par exemple, chiffrer en Rozier avec la clef MACLEF revient à chiffrer en Vigenère avec la clef OCJTBH. Cette nouvelle clef a été calculée ainsi:

```
                            1  -  13  +  1  =  -11
A - M + 1 = O            (=15)
C - A + 1 = C             3 -  1 + 1 =   3
L - C + 1 = J            12 -  3 + 1 =  10
E - L + 1 = T              5  -  12  + 1  =  -  6
F - E + 1 = B            (=20)
M - F + 1 = H             6 -  5 + 1 =   2
                         13 -  6 + 1 =   8
```

(la première colonne est la clef de Rozier décalée d'un cran vers le haut)

Le chiffre de Vigenère

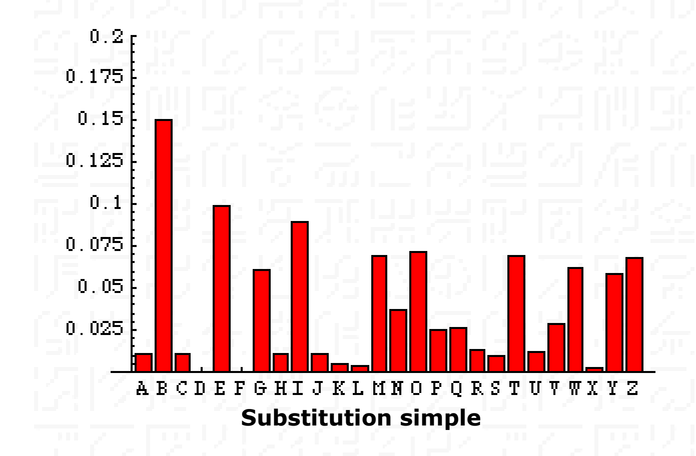


Blaise de Vigenère (1523-1596), diplomate français, se familiarisa avec les écrits d'Alberti, Trithème et Porta à Rome, où, âgé de vingt-six ans, il passa deux années en mission diplomatique. Au début, son intérêt pour la cryptographie était purement pratique et lié à son activité diplomatique. Une dizaine d'années plus tard, vers 1560, Vigenère considéra qu'il avait mis de côté assez d'argent pour abandonner sa carrière et se consacrer à l'étude. C'est seulement à ce moment-là qu'il examina en détail les idées de ses prédécesseurs, tramant grâce à elles un nouveau chiffre, cohérent et puissant. Bien qu'Alberti, Trithème, Bellaso et Porta en aient fourni les bases, c'est du nom de Vigenère que ce nouveau chiffre fut baptisé, en l'honneur de l'homme qui lui donna sa forme finale.
Le **chiffre de Vigenère** est une amélioration décisive du chiffre de César. Sa force réside dans l'utilisation non pas d'un, mais de 26 alphabets décalés pour chiffrer un message. On peut résumer ces décalages avec un carré de Vigenère. Ce chiffre utilise une clef qui définit le décalage pour chaque lettre du message (A: décalage de 0 cran, B: 1 cran, C: 2 crans, ..., Z: 25 crans).

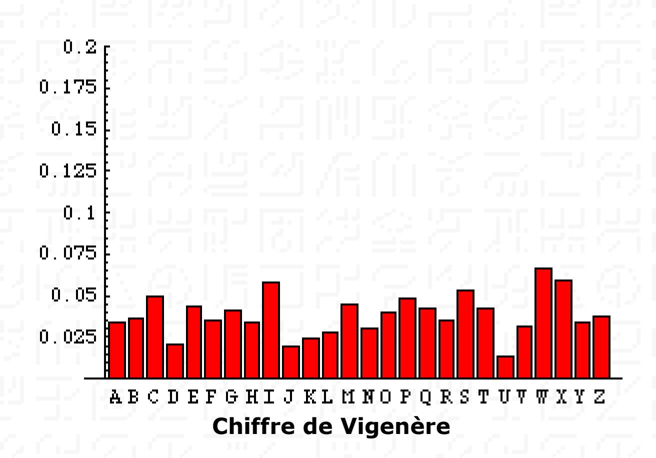
Exemple: chiffrons le texte "CHIFFRE DE VIGENERE" avec la clef "BACHELIER" (cette clef est éventuellement répétée plusieurs fois pour être aussi longue que le texte clair).

Clair	C	H	I	F	F	R	E	D	E	V	I	G	E	N	E	R	E
Clef	B	A	C	H	E	L	I	E	R	B	A	C	H	E	L	I	E
Décalage	1	0	2	7	4	11	8	4	17	1	0	2	7	4	11	8	4
Chiffré	D	H	K	M	J	C	M	H	V	W	I	I	L	R	P	Z	I

La grande force du chiffre de Vigenère est que la même lettre sera chiffrée de différentes manières. Par exemple le E du texte clair ci-dessus a été chiffré successivement M V L P I, ce qui rend inutilisable l'analyse des fréquences classique. Comparons les fréquences des lettres d'une fable de la Fontaine (Le chat, la belette et le petit lapin) chiffrée avec une substitution simple et celles de la même fable chiffrée avec le chiffre de Vigenère:



Substitution simple



Chiffre de Vigenère

On voit bien que l'histogramme n'a plus rien à voir avec celui d'une substitution simple: il est beaucoup plus "plat". Ce chiffre, qui a résisté trois siècles aux cryptanalystes, est pourtant relativement facile à casser, grâce à une méthode mise au point indépendamment par **Babagge** et **Kasiski**. Une autre méthode complètement différente a été encore mise au point plus tard par le commandant **Bazeries**.

Si la clef est aussi longue que le texte clair, et moyennant quelques précautions d'utilisation, le système est appelé masque jetable.

Exercices

Chiffrement



Chiffrez **à la main** le texte suivant avec le chiffre de Vigenère en utilisant le mot-clef "**Jeanne-Marie**":
Jeanne-Marie a des mains fortes, Mains sombres que l'été tanna

Déchiffrement

Déchiffrez **à la main** le texte suivant avec le chiffre de Vigenère en utilisant le mot-clef "**Jeanne-Marie**":

VEIAF TMLVA GXQMR QIEMR QRBQO EGIES FVXLI DRFQM IEAHN NUNAE

Vigenère sans clef secrète commune

Le chiffre de Vigenère tel que décrit ci-dessus exige, comme presque la totalité des systèmes de chiffrement, que les deux correspondants connaissent une clef secrète commune. Il est cepandant possible, moyennant trois envois de message au lieu d'un, de se passer de clef commune.

Tentez de trouver la manière de faire...

Le tableau de Trithème: Chiffres polyalphabétiques



Les Allemands et de nombreux auteurs de l'époque 1600-1700 prétendent que c'est l'abbé Trithème qui a inventé le carré de Vigenère. Un tel tableau (voir ci-contre) se trouve bien dans *Polygraphia*, mais il l'appelle «tableau de transposition» et ne l'emploie pas de la même façon que Vigenère. En outre, la notion de mot-clef est complètement absente de l'oeuvre de Trithème. C'est cependant bien la première fois qu'un tel tableau apparaît. Comment Trithème utilisait-il sa *tabula recta*? Il chiffrait la première lettre du message clair avec la première ligne, la deuxième lettre avec la deuxième ligne, etc. Il n'y avait pas d'alphabet clair distinct, mais la première ligne du tableau pouvait en tenir lieu. Quand il arrivait à la dernière ligne du tableau, il recommençait avec la première ligne. Cela revenait en fait à une suite de décalages de César: la première lettre n'était pas décalée, la deuxième était décalé d'un cran dans l'alphabet, la troisième de deux crans, etc., comme le montre le tableau ci-contre.

a b c d e f g h i k l m n o p q r s t u x y z
b c d e f g h i k l m n o p q r s t u x y z w
c d e f g h i k l m n o p q r s t u x y z w a
d e f g h i k l m n o p q r s t u x y z w a b
e f g h i k l m n o p q r s t u x y z w a b c
f g h i k l m n o p q r s t u x y z w a b c d
g h i k l m n o p q r s t u x y z w a b c d e
h i k l m n o p q r s t u x y z w a b c d e f
i k l m n o p q r s t u x y z w a b c d e f g
k l m n o p q r s t u x y z w a b c d e f g h
l m n o p q r s t u x y z w a b c d e f g h i
m n o p q r s t u x y z w a b c d e f g h i k
n o p q r s t u x y z w a b c d e f g h i k l
o p q r s t u x y z w a b c d e f g h i k l m
p q r s t u x y z w a b c d e f g h i k l m n
q r s t u x y z w a b c d e f g h i k l m n o
r s t u x y z w a b c d e f g h i k l m n o p
s t u x y z w a b c d e f g h i k l m n o p q
t u x y z w a b c d e f g h i k l m n o p q r
u x y z w a b c d e f g h i k l m n o p q r s
x y z w a b c d e f g h i k l m n o p q r s t
y z w a b c d e f g h i k l m n o p q r s t u
z w a b c d e f g h i k l m n o p q r s t u x
w a b c d e f g h i k l m n o p q r s t u x y

In hac tabula literarū canonica ſiue recta tot ex uno & uſuali noſtro latinarum literarum ipſarum per mutationem ſeu tranſpoſitionē habes alphabeta, quot in ea per totum ſunt monogrammata, uidelicet quater & uigeſies quatuor & uiginti, quæ faciunt in numero D.lxxvi. ac per totidē multiplicata, paulo efficiunt minus q̄ quatuordecēmilia.

o ij

Texte et traduction

In hac tabula literarum canonica sive recta tot ex uno et usuali nostro latinarum ipsarum per mutationem seu transpositionem habes alphabeta, quot in ea per totum sunt monogrammata, videlicet quater et vigesies quatuor et viginti, quae faciunt in numero D.IXXVI. ac per totidem multiplicata, paulo efficiunt minus quam quatuordecemmilia.

Sur ce tableau régulier ou carré de lettres, on trouve, par permutation ou transposition, l'alphabet usuel de nos lettres latines; or, on trouve sur ce tableau tout autant de monogrammes, à savoir 24 fois 24, qui font en nombre 576, et multiplié par autant (24), font un peu moins de 14'000.

Exemple: chiffrons le texte "CHIFFRE DE TRITHEME"

Message clair	C	H	I	F	F	R	E	D	E	T	R	I	T	H	E	M	E
Décalage	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Message chiffré	C	I	K	I	J	W	K	K	M	C	B	T	F	U	S	B	U

Exercice



Chiffrement

Chiffrez **à la main** le texte suivant avec le chiffre de Trithème:

> Mon coeur ne sait plus distinguer entre l'appât et le piège

Vérifiez votre cryptogramme avec le programme ci-dessus.

Déchiffrement

Déchiffrez **à la main** le texte suivant avec le chiffre de Trithème:

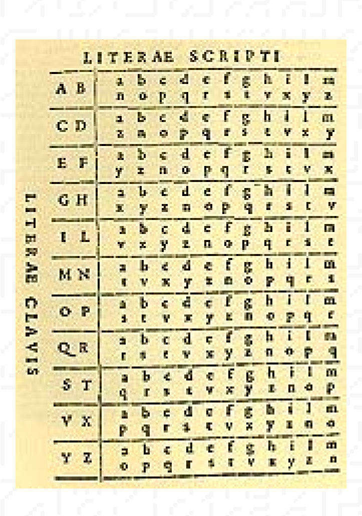
> NPWVW TSTMB WTQHL RKZLL XVJPS MEUCY IWTLY DONDH GSQEK NHHKK YRTFT H

Le chiffre de Porta

Le physicien italien **Giovanni Battista Della Porta** fut l'inventeur du premier système littéral à double clef, c'est-à-dire le premier chiffre pour lequel on change d'alphabet à chaque lettre. Ce système polyalphabétique était extrêmement robuste pour l'époque, à tel point que beaucoup considèrent Porta comme le "père de la cryptographie moderne". Della Porta a inventé son système de chiffrement en 1563, et il a été utilisé avec succès pendant trois siècles.

Porta emploie 11 alphabets différents et réversibles qu'il désigne, comme on le voit ci-dessous dans le tableau de droite, par AB, CD, EF, etc. Ce tableau peut être étendu à 13 alphabets (voir le tableau bleu de gauche), afin de pouvoir chiffrer toutes les lettres de notre alphabet occidental actuel.





LITERAE SCRIPTI

LITERAE CLAVIS

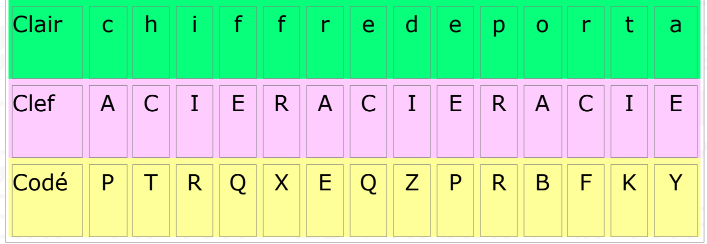
A B	a	b	c	d	e	f	g	h	i	l	m
	n	o	p	q	r	s	t	v	x	y	z
C D	a	b	c	d	e	f	g	h	i	l	m
	z	n	o	p	q	r	s	t	v	x	y
E F	a	b	c	d	e	f	g	h	i	l	m
	y	z	n	o	p	q	r	s	t	v	x
G H	a	b	c	d	e	f	g	h	i	l	m
	x	y	z	n	o	p	q	r	s	t	v
I L	a	b	c	d	e	f	g	h	i	l	m
	v	x	y	z	n	o	p	q	r	s	t
M N	a	b	c	d	e	f	g	h	i	l	m
	t	v	x	y	z	n	o	p	q	r	s
O P	a	b	c	d	e	f	g	h	i	l	m
	s	t	v	x	y	z	n	o	p	q	r
Q R	a	b	c	d	e	f	g	h	i	l	m
	r	s	t	v	x	y	z	n	o	p	q
S T	a	b	c	d	e	f	g	h	i	l	m
	q	r	s	t	v	x	y	z	n	o	p
V X	a	b	c	d	e	f	g	h	i	l	m
	p	q	r	s	t	v	x	y	z	n	o
Y Z	a	b	c	d	e	f	g	h	i	l	m
	o	p	q	r	s	t	v	x	y	z	n

Si on veut chiffrer avec un de ces alphabets, on choisit pour remplacer la lettre du texte clair la lettre qui lui fait face dans le tableau. Par exemple, si l'on chiffre avec l'alphabet AB, on substituera *a* par *n*, *b* par *o*, *q* par *d*, etc.
Ce chiffre est réversible: si on chiffre un texte déjà chiffré (avec la même clef bien sûr), on obtient à nouveau le texte clair.

Pour ne pas obliger les correspondants à prendre les onze alphabets à la suite, Porta propose de n'en adopter que cinq ou six et de convenir d'un mot-clef dont les lettres indiqueront les alphabets qu'il faudra successivement choisir. Ce mot constitue la clef du cryptogramme.

AB	a	b	c	d	e	f	g	h	i	j	k	l	m
	n	o	p	q	r	s	t	u	v	w	x	y	z
CD	a	b	c	d	e	f	g	h	i	j	k	l	m
	z	n	o	p	q	r	s	t	u	v	w	x	y
EF	a	b	c	d	e	f	g	h	i	j	k	l	m
	y	z	n	o	p	q	r	s	t	u	v	w	x
GH	a	b	c	d	e	f	g	h	i	j	k	l	m
	x	y	z	n	o	p	q	r	s	t	u	v	w
IJ	a	b	c	d	e	f	g	h	i	j	k	l	m
	w	x	y	z	n	o	p	q	r	s	t	u	v
KL	a	b	c	d	e	f	g	h	i	j	k	l	m
	v	w	x	y	z	n	o	p	q	r	s	t	u
MN	a	b	c	d	e	f	g	h	i	j	k	l	m
	u	v	w	x	y	z	n	o	p	q	r	s	t
OP	a	b	c	d	e	f	g	h	i	j	k	l	m
	t	u	v	w	x	y	z	n	o	p	q	r	s
QR	a	b	c	d	e	f	g	h	i	j	k	l	m
	s	t	u	v	w	x	y	z	n	o	p	q	r
ST	a	b	c	d	e	f	g	h	i	j	k	l	m
	r	s	t	u	v	w	x	y	z	n	o	p	q
	a	b	c	d	e	f	g	h	i	j	k	l	m

Par exemple, si le mot-clef est *ACIER*, on utilisera successivement les alphabets *A*, *C*, *I*, *E*, *R*, *A*, *C*, etc. pour chiffrer le message. Si l'on chiffre la phrase "chiffre de Porta" avec la clef *ACIER*, on obtiendra:



Clair	c	h	i	f	f	r	e	d	e	p	o	r	t	a
Clef	A	C	I	E	R	A	C	I	E	R	A	C	I	E
Codé	P	T	R	Q	X	E	Q	Z	P	R	B	F	K	Y

Pour déchiffrer, c'est le même principe: *F* devient *s*, *Z* devient *a*, etc.

Comme on le verra en exercice, il est déconseillé d'utiliser un alphabet régulier comme indiqué ci-dessus (a b c d e ...). Il vaut mieux utiliser des alphabets composés des 26 lettres réparties aléatoirement. Porta le recommandait déjà lui-même dans son traité *«De furtivis litterarum notis, vulgo de ziferis; Naples 1563»*.

C'est seulement en 1863 que le cryptologue allemand **Kasiski** découvrit comment casser le chiffre de Porta. Système désormais classique s'il en est: recherche de la longueur de la clef, puis ensuite analyse des fréquences (voir la page "Décryptement du chiffre de Vigenère"). Mais avec des clefs de grandes tailles, ce système est réellement sûr (à moins que le message soit vraiment très long).

Exercice

Chiffrement

Chiffrez **à la main** le texte suivant avec le chiffre de Porta en utilisant la clef "sed non satiata":

> Bizarre déité, brune comme les nuits,
> Au parfum mélangé de musc et de havane

Vérifiez votre cryptogramme avec le programme ci-dessus.

Déchiffrement

Déchiffrez **à la main** le texte suivant avec le chiffre de Porta en utilisant la clef "sed non satiata":

> KPIBL YURML RPDDP CVOSV SRLFC QVWZL TBRAV JBAPZ PFYTA WYREP URSPB YXGWN JKQVF JDUKM TZADR GB

Décryptement

Le chiffre de Porta tel qu'il est décrit sur cette page n'est pas très sûr. Le fait qu'une lettre appartenant à la première moitié de l'alphabet est forcément remplacée par une lettre de la deuxième moitié (et vice versa) est une faille que l'on peut exploiter (à vous de voir comment).
Décryptez le message suivant, sachant qu'il contient le mot "division":

> SRMYT EPFOG CBYAH ZXZYF TLIRJ HXJDJ MYTAT PSRWZ XRPAT TYDVR

Le chiffre de Beaufort



Le chiffre de l'amiral anglais **Sir Francis Beaufort** (1774-1857) fut publié après sa mort par son frère. Il semblerait que ce chiffre ait en fait été inventé par **Jean Sestri** vers 1710.
Beaufort (voir portrait ci-contre) est surtout resté célèbre pour son échelle des vents, qui classe les vents selon leur effet sur terre et sur mer sur une échelle de 0 (calme plat) à 12 (ouragan). De plus, une mer porte son nom.

Le chiffre de Beaufort est une variante du chiffre de Vigenère. Il utilise le carré de Vigenère d'une autre manière. Au lieu d'additionner la clef au message clair, Beaufort soustrait le message clair de la clef.

Il existe aussi une variante à l'allemande du chiffre de Beaufort.

Exemple

Chiffrons le texte "CHIFFRE DE BEAUFORT" avec la clef "BACHELIER" (les couleurs correspondent ici à celles utilisées dans le carré de Vigenère).

Clef	B	A	C	H	E	L	I	E	R	B	A	C	H	E	L	I	E
Clair	C	H	I	F	F	R	E	D	E	B	E	A	U	F	O	R	T
Décalage	-2	-7	-8	-5	-5	-17	-4	-3	-4	-1	-4	0	-20	-5	-14	-17	-19
Chiffré	Z	T	U	C	Z	U	E	B	N	A	W	C	N	Z	X	R	L

Exercice

Chiffrement

Chiffrez **à la main** le texte suivant avec le chiffre de Beaufort en utilisant le mot-clef "**Omar Khayyam**":

> Bois de ce vin, c'est la vie éternelle;
> C'est ce qui reste en toi des juvéniles délices; bois !

Vérifiez votre cryptogramme avec le programme ci-dessus.

Déchiffrement

Déchiffrez **à la main** le texte suivant avec le chiffre de Beaufort en utilisant le mot-clef "**Omar Khayyam"**:

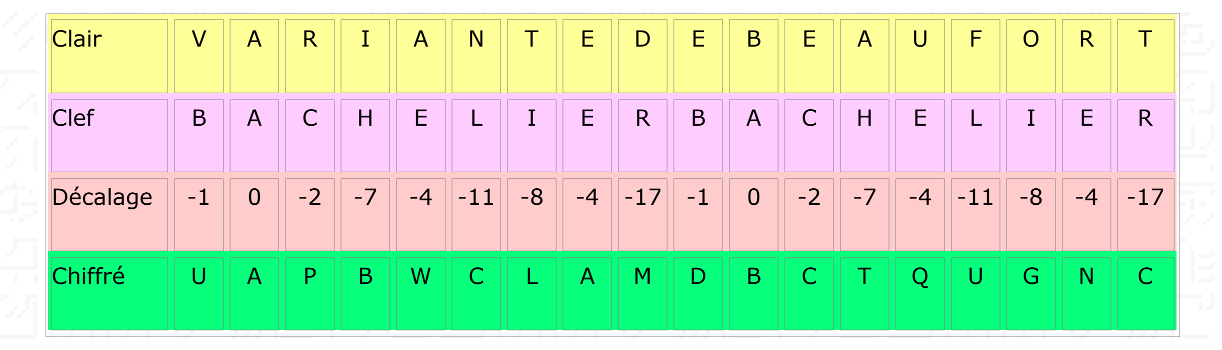
> GBZAQ WWWKO AKBWM GNOYQ IBKUH ACPHU GIIWE PGGPY RYNGK INNKN FQFAB KLMJS

Chiffre de Beaufort: la variante à l'allemande

Au lieu d'additionner la clef au message clair, comme on le fait dans le chiffre de Vigenère, la variante à l'allemande du chiffre de Beaufort soustrait la clef du message clair.

Exemple

Chiffrons le texte "VARIANTE DE BEAUFORT" avec la clef "BACHELIER" (les couleurs correspondent ici à celles utilisées dans le carré de Vigenère).



Clair	V	A	R	I	A	N	T	E	D	E	B	E	A	U	F	O	R	T
Clef	B	A	C	H	E	L	I	E	R	B	A	C	H	E	L	I	E	R
Décalage	-1	0	-2	-7	-4	-11	-8	-4	-17	-1	0	-2	-7	-4	-11	-8	-4	-17
Chiffré	U	A	P	B	W	C	L	A	M	D	B	C	T	Q	U	G	N	C

Exercice

Chiffrement

Chiffrez **à la main** le texte suivant avec la variante à l'allemande du chiffre de Beaufort en utilisant le mot-clef "Silhouette":

Donnez-moi des bijoux de noyées
Deux crèches

Vérifiez votre cryptogramme avec le programme ci-dessus.

Déchiffrement

Déchiffrez **à la main** le texte suivant avec la variante à l'allemande du chiffre de Beaufort en utilisant le mot-clef "Silhouette":

CFTID KHLLP CFTFM XKAAA LWBHP OOALA VKJBF KLHYZ WFCXL SKP

Chapitre XIX: Le crime de Tijuco

À l'arrivée du juge, tout le funèbre cortège s'était arrêté.

Un immense écho avait répété après lui et répétait encore ce cri qui s'échappait de toutes les poitrines :

"Innocent ! innocent !"

Puis, un silence complet s'établit.

On ne voulait pas perdre une seule des paroles qui allaient être prononcées.

Le juge Jarriquez s'était assis sur un banc de pierre, et là, pendant que Minha, Benito, Manoel, Fragoso l'entouraient, tandis que Joam Dacosta retenait Yaquita sur son cœur, il reconstituait tout d'abord le dernier paragraphe du document au moyen du nombre, et, à mesure que les mots se dégageaient nettement sous le chiffre qui substituait la véritable lettre à la lettre cryptologique, il les séparait, il les ponctuait, il lisait à haute voix.

Et voici ce qu'il lut au milieu de ce profond silence :

Le véritable auteur du vol des diamants et de

43 251343251 343251 34 325 134 32513432 51 34

Ph yjslyddqf dzxgas gz zqq ehx gkfndrxu ju gi

l'assassinat des soldats qui escortaient le convoi

32513432513 432 5134325 134 32513432513 43 251343

ocytdxvksbx hhu ypohdvy rym huhpuydkjox ph etozsl

commis dans la nuit du vingt-deux janvier mil huit

251343 2513 43 2513 43 251343251 3432513 432 5134

etnpmv ffov pd pajx hy ynojyggay meqynfu qln mvly

cent vingt-six, n'est donc pas Joam Dacosta, injustement

3251 34325134 3251 3432 513 4325 1343251 34325134325

fgsu zmqiztlb qgyu gsqe ubv nrcr edgruzb lrmxyuhqhpz

condamné à mort ; c'est moi, le misérable employé de

13432513 4 3251 3432 513 43 251343251 3432513 43

drrgcroh e pqxu fivv rpl ph onthvddqf hqsntzh hh

l'administration du district diamantin ; oui, moi seul,

251343251343251 34 32513432 513432513 432 513 4325

nfepmqkyuuexkto gz gkyuumfv ijdqdpzjq syk rpl xhxq

qui signe de mon vrai nom, Ortega.

134 32513 43 251 3432 513 432513

rym vkloh hh oto zvdk spp suvjhd.

Cette lecture n'avait pu être achevée, sans que d'interminables hurrahs se fussent élevés dans l'air.

Quoi de plus concluant, en effet, que ce dernier paragraphe qui résumait le document tout entier, qui proclamait si absolument l'innocence du fazender d'Iquitos, qui arrachait au gibet cette victime d'une effroyable erreur judiciaire !

Joam Dacosta, entouré de sa femme, de ses enfants, de ses amis, ne pouvait suffire à presser les mains qui se tendaient vers lui. Quelle que fût l'énergie de son caractère, la réaction se faisait, des larmes de joie s'échappaient de ses yeux, et en même temps son cœur reconnaissant s'élevait vers cette Providence qui venait de le sauver si miraculeusement, au moment, où il allait subir la dernière expiation, vers ce Dieu qui n'avait pas voulu laisser s'accomplir ce pire des crimes, la mort d'un juste !

Oui ! la justification de Joam Dacosta ne pouvait plus soulever aucun doute ! Le véritable auteur de l'attentat de Tijuco avouait lui-même son crime, et il dénonçait toutes les circonstances dans lesquelles il s'était accompli ! En effet, le juge Jarriquez, au moyen du nombre, venait de reconstituer toute la notice cryptogrammatique.

Or, voici ce qu'avouait Ortega.

Ce misérable était le collègue de Joam Dacosta, employé comme lui, à Tijuco, dans les bureaux du gouverneur de l'arrayal diamantin. Le jeune commis, désigné pour accompagner le convoi à Rio de Janeiro, ce fut lui. Ne reculant pas à cette horrible idée de s'enrichir par l'assassinat et le vol, il avait indiqué aux contrebandiers le jour exact où le convoi devait quitter Tijuco.

Pendant l'attaque des malfaiteurs qui attendaient le convoi au-delà de Villa-Rica, il feignit de se défendre avec les soldats de l'escorte ; puis, s'étant jeté parmi les morts, il fut emporté par ses complices, et c'est ainsi que le soldat, qui survécut seul à ce massacre, put affirmer qu'Ortega avait péri dans la lutte.

Mais le vol ne devait pas profiter au criminel, et, peu de temps après, il était dépouillé à son tour par ceux qui l'avaient aidé à commettre le crime.

Resté sans ressources, ne pouvant plus rentrer à Tijuco, Ortega s'enfuit dans les provinces du nord du Brésil, vers ces districts du Haut-Amazone où se trouvait la milice des "capitaës do mato". Il fallait vivre. Ortega se fit admettre dans cette peu honorable troupe. Là, on ne demandait ni qui on était, ni d'où l'on venait. Ortega se fit donc capitaine des bois, et, pendant de longues années, il exerça ce métier de chasseur d'hommes.

Sur ces entrefaites, Torrès, l'aventurier, dépourvu de tout moyen d'existence, devint son compagnon. Ortega et lui se lièrent intimement. Mais, ainsi que l'avait dit Torrès, le remords vint peu à peu troubler la vie du misérable. Le souvenir de son crime lui fit horreur. Il savait qu'un autre avait été condamné à sa place ! Il savait que cet autre, c'était son collègue Joam Dacosta ! Il savait enfin que, si cet innocent avait pu échapper au dernier supplice, il ne cessait pas d'être sous le coup d'une condamnation capitale !

Or, le hasard fit que, pendant une expédition de la milice, entreprise, il y avait quelques mois, au-delà de la frontière péruvienne, Ortega arriva aux environs d'Iquitos, et que là, dans Joam Garral, qui ne le reconnut pas, il retrouva Joam Dacosta.

Ce fut alors qu'il résolut de réparer, en la mesure du possible, l'injustice dont son ancien collègue était victime. Il consigna dans un document tous les faits relatifs à l'attentat de Tijuco ; mais il le fit sous la forme mystérieuse que l'on sait, son intention étant de le faire parvenir au fazender d'Iquitos avec le chiffre qui permettait de le lire.

La mort n'allait pas le laisser achever cette œuvre de réparation. Blessé grièvement dans une rencontre avec les noirs de la Madeira, Ortega se sentit perdu. Son camarade Torrès était alors près de lui. Il crut pouvoir confier à cet ami le secret qui avait si lourdement pesé sur toute son existence. Il lui remit le document écrit tout entier de sa main, en lui faisant jurer de le faire parvenir à Joam Dacosta, dont il lui donna le nom et l'adresse, et de ses lèvres s'échappa, avec son dernier soupir, ce nombre 432513, sans lequel le document devait rester absolument indéchiffrable.

Ortega mort, on sait comment l'indigne Torrès s'acquitta de sa mission, comment il résolut d'utiliser à son profit le secret dont il était possesseur, comment il tenta d'en faire l'objet d'un odieux chantage.

Torrès devait violemment périr avant d'avoir accompli son œuvre, et emporter son secret avec lui. Mais ce nom d'Ortega, rapporté par Fragoso, et qui était comme la signature du document, ce nom avait enfin permis de le reconstituer, grâce à la sagacité du juge Jarriquez.

Oui ! c'était là la preuve matérielle tant cherchée, c'était l'incontestable témoignage de l'innocence de Joam Dacosta, rendu à la vie, rendu à l'honneur !

Les hurrahs redoublèrent lorsque le digne magistrat eut, à haute voix et pour l'édification de tous, tiré du document cette

terrible histoire.

Et, dès ce moment, le juge Jarriquez, possesseur de l'indubitable preuve, d'accord avec le chef de la police, ne voulut pas que Joam Dacosta, en attendant les nouvelles instructions qui allaient être demandées à Rio de Janeiro, eût d'autre prison que sa propre demeure.

Cela ne pouvait faire difficulté, et ce fut au milieu du concours de la population de Manao que Joam Dacosta, accompagné de tous les siens, se vit porté plutôt que conduit jusqu'à la maison du magistrat comme un triomphateur.

En ce moment, l'honnête fazender d'Iquitos était bien payé de tout ce qu'il avait souffert pendant de si longues années d'exil, et, s'il en était heureux, pour sa famille plus encore que pour lui, il était non moins fier pour son pays que cette suprême injustice n'eût pas été définitivement consommée !

Et, dans tout cela, que devenait Fragoso ?

Eh bien ! l'aimable garçon était couvert de caresses ! Benito, Manoel, Minha l'en accablaient, et Lina ne les lui épargnait pas ! Il ne savait à qui entendre, et il se défendait de son mieux ! Il n'en méritait pas tant ! Le hasard seul avait tout fait ! Lui devait-on même un remerciement, parce qu'il avait reconnu en Torrès un capitaine des bois ? Non, assurément. Quant à l'idée qu'il avait eue d'aller rechercher la milice à laquelle Torrès avait appartenu, il ne semblait pas qu'elle pût améliorer la situation, et, quant à ce nom d'Ortega, il n'en connaissait même pas la valeur !

Brave Fragoso ! Qu'il le voulût ou non, il n'en avait pas moins sauvé Joam Dacosta !

Mais, en cela, quelle étonnante succession d'événements divers, qui avaient tous tendu au même but : la délivrance de Fragoso, au moment où il allait mourir d'épuisement dans la forêt d'Iquitos, l'accueil hospitalier qu'il avait reçu à la fazenda, la rencontre de Torrès à la frontière brésilienne, son embarquement sur la jangada, et, enfin, cette circonstance que Fragoso l'avait déjà vu quelque part !

"Eh bien, oui ! finit par s'écrier Fragoso, mais ce n'est pas à moi qu'il faut rapporter tout ce bonheur, c'est à Lina !

- À moi ! répondit la jeune mulâtresse.

- Eh, sans doute ! sans la liane, sans l'idée de la liane, est-ce que j'aurais jamais pu faire tant d'heureux !"

Si Fragoso et Lina furent fêtés, choyés par toute cette honnête famille, par les nouveaux amis que tant d'épreuves leur avaient faits à Manao, il est inutile d'y insister.

Mais le juge Jarriquez, n'avait-il pas sa part, lui aussi, dans cette réhabilitation de l'innocent ? Si, malgré toute la finesse de ses talents d'analyste, il n'avait pu lire ce document, absolument indéchiffrable pour quiconque n'en possédait pas la clef, n'avait-il pas du moins reconnu sur quel système cryptographique il reposait ? Sans lui, qui aurait pu, avec ce nom seul d'Ortega, reconstituer le nombre que l'auteur du crime et Torrès, morts tous les deux, étaient seuls à connaître ?

Aussi les remerciements ne lui manquèrent-ils pas !

Il va sans dire que, le jour même, partait pour Rio de Janeiro un rapport détaillé sur toute cette affaire, auquel était joint le document original, avec le chiffre qui permettait de le lire. Il fallait attendre que de nouvelles instructions fussent envoyées du ministère au juge de droit, et nul doute qu'elles n'ordonnassent l'élargissement immédiat du prisonnier.

C'était quelques jours à passer encore à Manao ; puis, Joam Dacosta et les siens, libres de toute contrainte, dégagés de toute inquiétude, prendraient congé de leur hôte, se rembarqueraient, et continueraient à descendre l'Amazone jusqu'au Para, où le voyage devait se terminer par la double union de Minha et de Manoel, de Lina et de Fragoso, conformément au programme arrêté avant le départ.

Quatre jours après, le 4 septembre, arrivait l'ordre de mise en liberté. Le document avait été reconnu authentique. L'écriture en était bien celle de cet Ortega, l'ancien employé du district diamantin, et il n'était pas douteux que l'aveu de son crime, avec les plus minutieux détails qu'il en donnait, n'eût été entièrement écrit de sa main.

L'innocence du condamné de Villa-Rica était enfin admise. La réhabilitation de Joam Dacosta était judiciairement reconnue.

Le jour même, le juge Jarriquez dînait avec la famille à bord de la jangada, et, le soir venu, toutes les mains pressaient les siennes. Ce furent de touchants adieux ; mais ils comportaient l'engagement de se revoir à Manao, au retour, et, plus tard, à la fazenda d'Iquitos.

Le lendemain matin, 5 septembre, au lever du soleil, le signal du départ fut donné. Joam Dacosta, Yaquita, leur fille, leurs fils, tous étaient sur le pont de l'énorme train. La jangada, démarrée, commença à prendre le fil du courant, et, lorsqu'elle disparut au tournant du rio Negro, les hurrahs de toute la population, pressée sur la rive, retentissaient encore.

Le chiffre de Gronsfeld

Le Belge José de Bronckhorst, **Comte de Gronsfeld**, était un homme de guerre, mais aussi un diplomate. Sa situation lui imposait de garder certains renseignements secrets. Vers 1734, il mit au point son propre système de chiffrage: une amélioration du chiffre de César utilisant un décalage variable donné sous forme d'une clef numérique. Par exemple, si l'on chiffre la phrase "chiffre de Gronsfeld" avec la clé numérique "1734", on obtiendra:

Clair	C	H	I	F	F	R	E	D	E	G	R	O	N	S	F	E	L	D
Clef (décalages)	1	7	3	4	1	7	3	4	1	7	3	4	1	7	3	4	1	7
Chiffré	D	O	L	J	G	Y	H	H	F	N	U	S	O	Z	I	I	M	K

Ce système est en fait une variante du chiffre de Vigenère, la différence étant qu'il n'y a que 10 décalages possibles au lieu de 26.

La méthode pour décrypter un message chiffré avec le chiffre de Gronsfeld est la même que celle utilisée pour décrypter le système de Vigenère.

Travail (décryptement)

Le chiffre de Gronsfeld est utilisé dans le livre de Jules Verne "La Jangada". Pour le décrypter, le juge Jarriquez a recours au procédé du **mot probable**. Il a en effet supposé que l'auteur du message, un dénommé Ortega, avait signé son texte.

> "Phxjslxddqfdywgzsgyyqqehwgkfndrwujugiocxtdwvksbwhhuxpohdvxrxmhuhpuxdkj
> owphetoysletnpmvffovpdpzjwhxxnojxggzymeqxnfuqlnmvlxfgsuymqiytlbqgxugsqeub
> vnrcredgruyblrmwxuhqhpydrrgcrohepqwufivvrplphonthvddqfhqsntzhhhnfepmqkxuu
> ewktogygkxuumfvijdqdpyjqsxkrplwhwqrxmvklohhhotoyvdksppsuvjhd"

Trouvez la clef de chiffrement et décryptez ce texte ! La réponse se trouve dans le roman (deuxième partie, chapitre 19): La Jangada, de Jules Verne

---

Masque jetable

Le masque jetable est le seul algorithme de cryptage connu comme étant indécryptable. C'est en fait un chiffre de Vigenère avec comme caractéristique que la clef de chiffrement a la même longueur que le message clair. Le système du masque jetable fut inventé par **Gilbert Vernam** en 1917, puis perfectionné par le major **Joseph O. Mauborgne** en 1918, qui inventa le concept de clef aléatoire.

Clair	M	A	S	Q	U	E	J	E	T	A	B	L	E
Clef	X	C	A	A	T	E	L	P	R	V	G	Z	C
Décalage	23	2	0	0	19	4	11	15	17	21	6	25	2
Chiffré	J	C	S	Q	N	I	U	T	K	V	H	K	G


Vernam


Mauborgne

Méthode du masque jetable

Pour chiffrer un texte de manière sûre avec le chiffre de Vigenère, vous devez:

1. choisir une clef aussi longue que le texte à chiffrer,
2. utiliser une clef formée d'une suite de caractères aléatoires,
3. protéger votre clef,
4. ne jamais réutiliser une clef,
5. écrire des textes clairs ne contenant que les lettres (sans ponctuation et sans espaces).

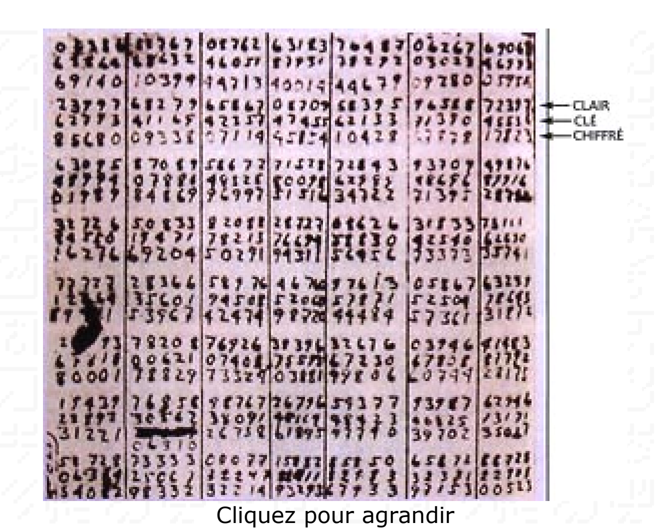
Le problème de ce système est de communiquer les clefs de chiffrage ou de trouver un algorithme de génération de clef commun aux deux partenaires. Un algorithme à base de cartes à jouer a été proposé récemment par Bruce Schneier: le Solitaire.

Le système du masque jetable, avec les précautions indiquées ci-dessus, est absolument inviolable si l'on ne connaît pas la clef. Il est couramment utilisé de nos jours par les États. En effet, ceux-ci peuvent communiquer les clefs à leurs ambassades de manière sûre via la valise diplomatique.

Lorsqu'en 1967 l'armée bolivienne captura et exécuta le révolutionnaire Che Guevara, les militaires trouvèrent sur son corps un papier montrant comment il préparait les messages qu'il voulait transmettre au président cubain Fidel Castro. Le Che utilisait le chiffre incassable inventé par Vernam. Les lettres du message du Che (rédigé en espagnol) étaient d'abord transformées en nombres décimaux selon la règle de substitution fixe suivante:

Clair	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Chiffré	6	38	32	4	8	30	36	34	39	31	78	72	70	76	9	79	71	58	2	0	52	50	56	54	1	59

En elle-même, cette substitution ne procure aucune protection. Les chiffres du message mis à la suite sont ensuite découpés en blocs de cinq chiffres: c'est la ligne supérieure que l'on voit sur le document ci-dessous. La ligne du milieu est la clef, une séquence aléatoire de chiffres connue uniquement du Che et de Fidel Castro. Ensuite, le message et la clef sont additionnés (sans retenue, i.e. modulo 10), ce qui donne le message chiffré, la ligne inférieure de chaque groupe de trois lignes.
Pour déchiffrer, il fallait prendre le message chiffré, lui soustraire (modulo 10) la clef, puis faire la substitution inverse pour traduire les chiffres en lettres.



Cliquez pour agrandir


Fidel Castro et Che Guevara

Exercice:

Déchiffrement

Le message ci-dessous a été chiffré avec le chiffre du Che. La clef est le nombre π. Déchiffrez-le !

01237 55235 31127 12189 87479 1592

Décryptement

L'auteur des deux messages chiffrés ci-dessous n'a pas pris toutes les précautions qui s'imposent pour la sécurité totale du masque jetable: il a utilisé deux fois la même clef et de plus cette clef n'est pas aléatoire. Décryptez les messages ci-dessous, en essayant le mot probable "ennemi".

MYRWF AISPR AKOAL IOPHT LWUHP LZOWT WEWTR FOSFI FEJSC HJJD

ICXAE DMOPI YERWM CGAWN VREHP LZOWT WHHMN FOSFI UTKEB YWIPP UMAPH MHV

Procédé autoclave

Un procédé **autoclave** utilise le message clair lui-même comme clef. Prenons par exemple un message que nous allons chiffrer avec le chiffre de Vigenère. Comme clef, vous allons utiliser le message lui-même, précédé de la lettre X (on aurait évidemment pu prendre n'importe quel mot pour commencer la clef).

Exemple: chiffrons le texte "PRODEDE AUTOCLAVE" avec la clef "X PRODEDE AUTOCLAV".

Clair	P	R	O	C	E	D	E	A	U	T	O	C	L	A	V	E
Clef	X	P	R	O	C	E	D	E	A	U	T	O	C	L	A	V
Décalage	23	15	17	14	2	4	3	4	0	20	19	14	2	11	0	21
Chiffré	M	G	F	Q	G	H	H	E	U	N	H	Q	N	L	V	Z

Le grand problème de ce procédé est que si le message chiffré arrive avec des lacunes ou des erreurs, il deviendra indéchiffrable, en particulier si le début du message manque. Il offre en outre au cryptanalyste des facilités (par exemple, si le début de la clef est composé d'une seule lettre, il suffit de les essayer les 26; les lettres suivantes de la clef apparaîtront d'elles-mêmes au fur et à mesure du décryptement).

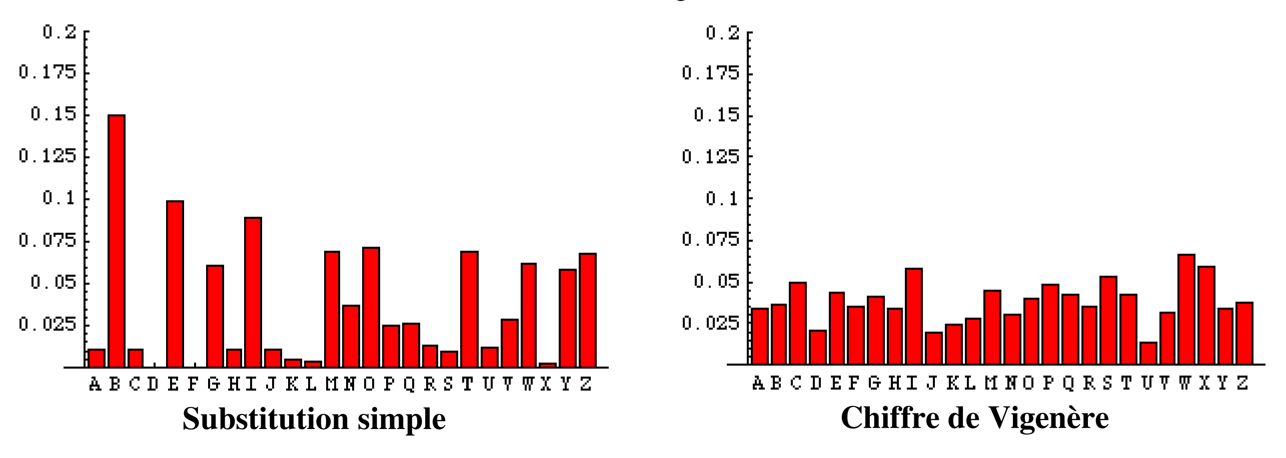
TD4: Vigenère, test de Friedman

1: Le chiffre de Vigenère

Blaise de Vigenère (1523-1596), diplomate français, se familiarisa avec les écrits d'Alberti, Trithème et Porta à Rome, où, âgé de vingt-six ans, il passa deux années en mission diplomatique. Au début, son intérêt pour la cryptographie était purement pratique et lié à son activité diplomatique. Une dizaine d'années plus tard, vers 1560, Vigenère considéra qu'il avait mis de côté assez d'argent pour abandonner sa carrière et se consacrer à l'étude. C'est seulement à ce moment-là qu'il examina en détail les idées de ses prédécesseurs, tramant grâce à elles un nouveau chiffre, cohérent et puissant. Bien qu'Alberti, Trithème, Bellaso et Porta en aient fourni les bases, c'est du nom de Vigenère que ce nouveau chiffre fut baptisé, en l'honneur de l'homme qui lui donna sa forme finale.
Le **chiffre de Vigenère** est une amélioration décisive du chiffre de César. Sa force réside dans l'utilisation non pas d'un, mais de 26 alphabets décalés pour chiffrer un message. On peut résumer ces décalages avec un carré de Vigenère. Ce chiffre utilise une **clef** qui définit le décalage pour chaque lettre du message (A: décalage de 0 cran, B: 1 cran, C: 2 crans, ..., Z: 25 crans).

La grande force du chiffre de Vigenère est que la même lettre sera chiffrée de différentes manières.

Comparons les fréquences des lettres d'un même texte chiffrée avec une substitution simple et celles de la même fable chiffrée avec le chiffre de Vigenère:



Substitution simple **Chiffre de Vigenère**

On voit bien que l'histogramme n'a plus rien à voir avec celui d'une substitution simple:

Il est beacup plus « plat ».

Ce chiffre, qui a résisté trois siècles aux cryptanalystes, est pourtant relativement facile à casser, grâce à une méthode mise au point indépendamment par **Babagge** et **Kasiski**. Une autre méthode complètement différente a été encore mise au point plus tard par le commandant **Bazeries**.

Si la clef est aussi longue que le texte clair, et moyennant quelques précautions d'utilisation, le système est appelé masque jetable.

Exercice 1:

Chiffrement

Chiffrez **à la main** le texte suivant avec le chiffre de Vigenère en utilisant le mot-clef "**Jeanne-Marie**":

> **Jeanne-Marie a des mains fortes,**
> **Mains sombres que l'été tanna**

Déchiffrement

Déchiffrez **à la main** le texte suivant avec le chiffre de Vigenère en utilisant le mot-clef "**Jeanne-Marie"**:

> **VEIAF TMLVA GXQMR QIEMR QRBQO EGIES FVXLI DRFQM IEAHN NUNAE**

Vigenère sans clef secrète commune

Le chiffre de Vigenère tel que décrit ci-dessus exige, comme presque la totalité des systèmes de chiffrement, que les deux correspondants connaissent une clef secrète commune. Il est cependant possible, moyennant trois envois de message au lieu d'un, de se passer de clef commune.
Tentez de trouver la manière de faire...

2: Le test de Friedman

Le **test de Friedman** (aussi appelé **test kappa**) s'appuie sur la métrique appelée Indice de Coïncidence (IC). Il a pour premier objectif de **déterminer si un texte a été chiffré avec un chiffre monoalphabétique ou polyalphabétique**. Comme second bénéfice, **il suggère la longueur du mot-clef si le chiffre est polyalphabétique**.

Comment trouver la longueur de la clef d'un chiffre de Vigenère

Soit le message suivant, chiffré avec Vigenère (369 lettres):

PERTQ UDCDJ XESCW MPNLV MIQDI ZTQFV XAKLR PICCP QSHZY DNCPW EAJWS ZGCLM QNRDE OHCGE ZTQZY HELEW AUQFR OICWH QMYRR UFGBY QSEPV NEQCS EEQWE EAGDS ZDCWE OHYDW QERLM FTCCQ UNCPP QSKPY FEQOI OHGPR EERWI EFSDM XSYGE UELEH USNLV GPMFV EIVXS USJPW HIEYS NLCDW MCRTZ MICYX MNMFZ QASLZ QCJPY DSTTK ZEPZR ECMYW OICYG UESIU GIRCE UTYTI ZTJPW HIEYI ETYYH USOFI XESCW HOGDM ZSNLV QSQPY JSCAV QSQLM QNRLP QSRLM XLCCG AMKPG QLYLY DAGEH GERCI RAGEI ZNMGI YBPP

On va considérer les sous-chaînes obtenues en prenant les lettres à intervalle donné:

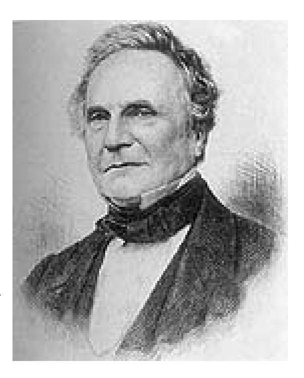
Intervalle de 1: PERTQ UDCDJ XESCW MPNLV ... (**texte original**)
Intervalle de 2: PRQDD XSWPL ... et ETUCJ ECMNV ...
Intervalle de 3: PTDJS MLIIQ ... , EQCXC PVQZF... et RUDEW NMDTV ...

On calcule ensuite les IC pour toutes ces sous-chaînes.

Intervalle	Indice de coïncidence
1	0.0456107
2	0.0476954, 0.0443098
3	0.044249, 0.0494469, 0.0426771
4	0.0465839, 0.0453894, 0.0449116, 0.0425227
5	0.0799704, 0.0925583, 0.0836727, 0.0795282, 0.0684932
6	0.0512956, 0.0407192, 0.0371585, 0.0382514, 0.0661202, 0.0431694

On remarque que quand l'intervalle est de 5, l'IC correspond plus ou moins avec l'IC caractéristique du français (en tout cas, c'est cette ligne qui s'approche le plus de 0.074, les autres lignes étant plutôt proches de 0.038). La longueur de la clef utilisée est donc probablement 5. Pour découvrir la clef elle-même, on peut ensuite procéder comme le faisait Kasiski (ceci est laissé en exercice).

Décryptement du chiffre de Vigenère (théorie)



La figure la plus étonnante de la cryptanalyse au XIXème siècle est celle de **Charles Babbage (1792-1871)**, fils d'un prospère banquier londonien . En matière de découvertes scientifiques, il fut le premier à comprendre que dans un tronc d'arbre, la largeur d'un anneau dépend du temps qu'il a fait dans l'année. Il s'intéressa aux statistiques (premières tables de mortalité). Il proposa un prix unique pour l'affranchissement d'une lettre. Après s'être rendu compte que les éphémérides nautiques pour trouver la latitude et la longitude en mer contenaient plus de mille erreurs, il échoua faute de financement à construire une machine mécanique capable de faire des calculs avec un haut degré de précision.

Il apporta une contribution importante à la cryptanalyse: il réussit à casser le chiffre de Vigenère, probablement en 1854 car sa découverte resta ignorée en l'absence d'écrit. Pendant ce temps, un officier prussien à la retraite, **Friedrich Wilhelm Kasiski (1805-1881),** parvint au même résultat et publia en **1863 "*Die Geheimschriftren und die Dechiffrir-kunst*"**.

Dans l'exemple ci-dessus, le mot **"thé"** est chiffré "**DPP"** 2 fois et "**BSS"** 1 fois.

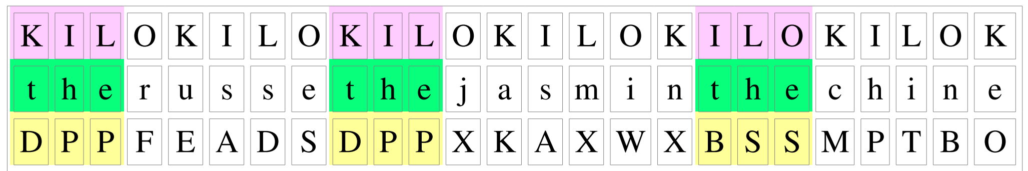
Babbage comprit que des répétitions de cette sorte lui offraient la prise dont il avait besoin pour attaquer Vigenère. Il va d'abord chercher des séquences de lettres qui apparaissent plus d'une fois dans le texte:

- **soit la même séquence de lettres du texte clair a été cryptée avec la même partie de la clef**
- **soit deux suites de lettres différentes dans le texte clair auraient (possibilité faible) par pure coïncidence engendré la même suite dans le texte chiffré.**

Le 1er cas étant le plus probable, il en déduit le nombre de facteurs de la clef puis par une méthode de fréquence de distribution des lettres cryptées il en déduit les lettres du texte clair.

En prenant par exemple la clef KILO, la lettre E peut être chiffrée en O, M, P ou S selon que K, I, L ou O sont utilisés pour la chiffrer. Ainsi le mot *thé* peut être chiffré en DPP, BSS, EVO ou HRM.

Exemple :



K	I	L	O	K	I	L	O	K	I	L	O	K	I	L	O	K	I	L	O	K	I	L	O	K
t	h	e	r	u	s	s	e	t	h	e	j	a	s	m	i	n	t	h	e	c	h	i	n	e
D	P	P	F	E	A	D	S	D	P	P	X	K	A	X	W	X	B	S	S	M	P	T	B	O

Dans cet exemple **THE** est chiffré en **DPP** la première et la deuxième fois, et en **BSS** la troisième. C'est pourtant la faiblesse du chiffre de Vigenère: ces répétitions apparaissent parce que dans l'original, les mêmes séquences de lettres sont chiffrées avec la même partie de la clef.

Un exemple complet

Texte chiffré :

```
KQOWE FVJPU JUUNU KGLME KJINM WUXFQ MKJBG WRLFN FGHUD WUUMB SVLPS
NCMUE KQCTE SWREE KOYSS IWCTU AXYOT APXPL WPNTC GOJBG FQHTD WXIZA
YGFFN SXCSE YNCTS SPNTU JNYTG GWZGR WUUNE JUUQE APYME KQHUI DUXFP
GUYTS MTFFS HNUOC ZGMRU WEYTR GKMEE DCTVR ECFBD JQCUS WVBPN LGOYL
SKMTE FVJJT WWMFM WPNME MTMHR SPXFS SKFFS TNUOC ZGMDO EOYEE KCPJR
GPMUR SKHFR SEIUE VGOYC WXIZA YGOSA ANYDO EOYJL WUNHA MEBFE LXYVL
WNOJN SIOFR WUCCE SWKVI DGMUC GOCRU WGNMA AFFVN SIUDE KQHCE UCPFC
MPVSU DGAVE MNYMA MVLFM AOYFN TQCUA FVFJN XKLNE IWCWO DCCUL WRIFT
WGMUS WOVMA TNYBU HTCOC WFYTN MGYTQ MKBBN LGFBT WOJFT WGNTE JKNEE
DCLDH WTVBU VGFBI JG
```

Il faut d'abord chercher des séquences de lettres qui apparaissent plus d'une fois dans le texte.

		Longueurs de clef possibles				
Séquence répétée	Espace de répétition	2	3	5	19	
WUU	95			x	x	
EEK	200	x		x		
WXIZAYG	190	x		x	x	
NUOCZGM	80	x		x		
DOEOY	45		x	x		
GMU	90	x	x	x		

Les facteurs premiers du nombre de caractères entre deux débuts de séquences figurent dans le tableau (ex. 95 = 5 x 19). Il apparaît dans le tableau que toutes les périodes sont divisibles par 5.

Tout se cale parfaitement sur un mot-clef de 5 lettres

Une autre méthode pour trouver la longueur de la clef utilise l'indice de coïncidence.

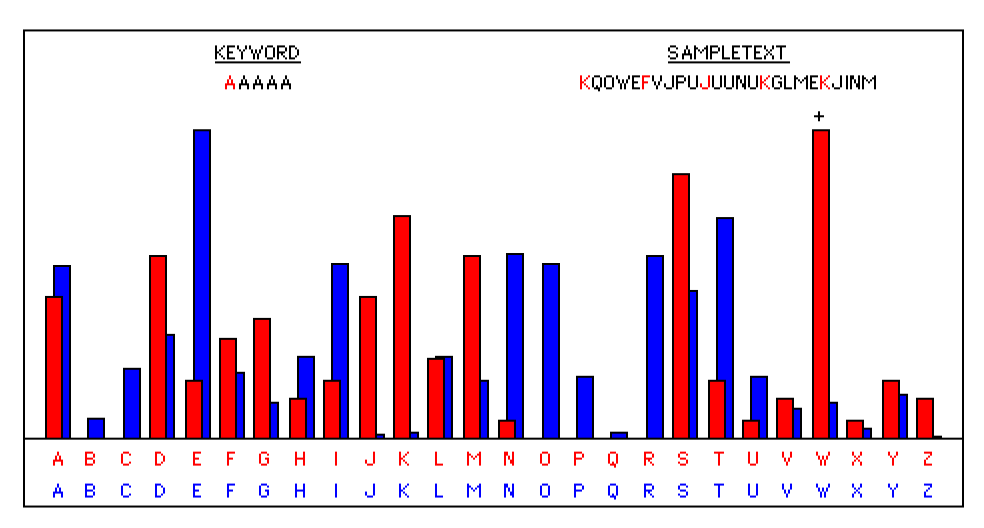
Il va falloir découvrir les lettres du mot clef : **L1-L2-L3-L4-L5,**

L1 représente la 1ère lettre du mot clef et ainsi de suite.

Commençons par déterminer L1

Nous savons que la ligne du carré de Vigenère, définie par L1, commande l'alphabet chiffré pour la 1ère, la 6ème, la 11ème ... lettres du message. En regardant la 1ère, la 6ème, la 11ème ... lettres du texte chiffré on peut utiliser la bonne vieille méthode de l'analyse des fréquences.

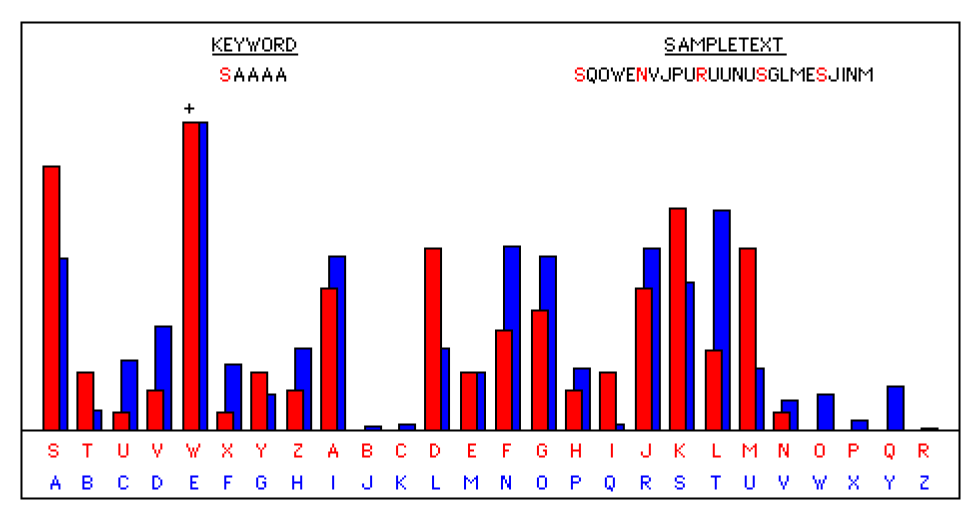
On trace, grâce à une applet spécialement conçue dans ce but, un graphique montrant la distribution des lettres qui apparaissent à la 1ère, la 6ème, la 11ème ... dans le texte chiffré **KQOWEFVJPUJUUNUKG ... , soit K, F, J, ...**



La répétition ci-dessus (en rouge) présente des traits communs avec celle de l'alphabet courant (en bleu) décalée de 18 crans. Le pic bleu le plus important se trouve sur le e et le pic rouge sur le W.

L1	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R

En superposant les deux graphiques pour qu'ils aient la même silhouette générale, nous constatons que la 1ère lettre du mot clef L1 est S.



Trouvons la clef complète

On recommence la même démarche pour identifier les autres lettres du mot-clef. On trouve pour chaque lettre L2, L3, L4 et L5 :

L2	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
L3	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
L4	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
L5	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Le mot-clef est: **S C U B A**

Texte clair:

Souvent pour s'amuser les hommes d'équipage prennent des albatros, vastes oiseaux des mers, qui suivent, indolents compagnons de voyage, le navire glissant sur les gouffres amers. A peine les ont-ils déposés sur les planches que ces rois de l'azur, maladroits et honteux, laissent piteusement leurs grandes ailes blanches, comme des avirons, traîner à côté d'eux. Ce voyageur ailé, comme il est gauche et veule, lui naguère si beau, qu'il est comique et laid. L'un agace son bec avec un brûle-gueule, l'autre mime en boitant l'infirme qui volait. Le poète est semblable au prince des nuées, qui hante la tempête et se rit de l'archer.

Baudelaire

Récapitulation sous forme d'exercice:

Décryptez le texte suivant:

XAUNM EESYI EDTLL FGSNB WQUFX PQTYO RUTYI INUMQ IEULS MFAFX GUTYB XXAGB HMIFI
IMUMQ IDEKR IFRIR ZQUHI ENOOO IGRML YETYO VQRYS IXEOK IYPYO IGRFB WPIYR BQURJ
IYEMJ IGRYK XYACP PQSPB VESIR ZQRUF REDYJ IGRYK XBLOP JARNP UGEFB WMILX MZSMZ
YXPNB PUMYZ MEEFB UGENL RDEPB JXONQ EZTMB WOEFI IPAHP PQBFL GDEMF WFAHQ

Pour attaquer un chiffre de Vigenère, il faut trouver la clef! Cela est possible si la clef est courte et le texte long. Le texte ci-dessus a été chiffré avec une clef trop courte. Dans ce cas des séquences de lettres peuvent apparaître plusieurs fois.

Expliquez pourquoi.

Le premier pas consiste à deviner la longueur de la clef. On cherche pour cela des séquences de plusieurs lettres consécutives (par exemple 3 ou plus) apparaissant plusieurs fois.

XAUNM EESYI EDTLL FGSNB WQUFX PQTYO RUTYI INUMQ IEULS MFAFX GUTYB XXAGB HMIFI
IMUMQ IDEKR IFRIR ZQUHI ENOOO IGRML YETYO VQRYS IXEOK IYPYO IGRFB WPIYR BQURJ
IYEMJ IGRYK XYACP PQSPB VESIR ZQRUF REDYJ IGRYK XBLOP JARNP UGEFB WMILX MZSMZ
YXPNB PUMYZ MEEFB UGENL RDEPB JXONQ EZTMB WOEFI IPAHP PQBFL GDEMF WFAHQ

D'après l'emplacement de ces groupes, déduisez la longueur de la clef.

Ce renseignement est capital. Si, par exemple, la longueur de la clef est 3, cela signifie que les caractères de rang **1, 4, 7, 10, ..., 3k+1, sont simplement décalés à la manière du chiffre de César.** On peut donc appliquer maintenant l'analyse de fréquences à ces caractères et trouver la première lettre de la clef. Pour la deuxième lettre de la clef, on analysera les fréquences des caractères de rang 3k+2 et pour le dernière lettre les fréquences des caractères de rang 3k.

Décryptez le texte. Qui a écrit ce poème?
